HEALTH LAW UPDATE

NPO PAAC Petoskey

November 14, 2017

By: LAURA M. DINON

PLUNKETT COONEY
ldinon@plunkettcooney
(231) 348-6417

HEALTH LAW 2017

I. Equal Employment Opportunity/Civil Rights in Health Care

See attached EEOC handouts.

II. Regulatory and Legal Update

A. Medicare Access and CHIP Reauthorization Act of 2015

1. On April 16, 2015, the Medicare Access and CHIP Reauthorization Act of 2015 (PL 114-10) was signed into law by President Obama ("MACRA"). MACRA made significant changes to how Medicare pays for physician services, creating a Quality Payment Program ("QPP") to better emphasize quality and efficiency. MACRA also:

(a) ends the Sustainable Growth Rate ("SGR") formula for determining Medicare payments for healthcare services;

(b) establishes a new framework for rewarding healthcare providers for giving better care; and

(c) creates one new quality reporting program system.

See, CMS.gov, Centers for Medicare & Medicaid Services, MACRA: MIPS & APMs, at https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/MACRA-MIPS-and-APMs/MACRA-MIPS-and-APMs.html.

2. MACRA sunsets several existing programs on the last day of 2018, including:

a. the meaningful use incentive program for certified Electronic Health Record ("EHR") technology; the physician quality reporting system; and the value-based payment modifier. In their place, the merit-based incentive payment system ("MIPS") will be established, to:

(1) develop a methodology to assess the total performance of each MIPS-eligible professional according to performance standards;

(2) use the methodology to provide a composite performance score for each professional for each performance period; and

(3) use the composite performance score of the MIPS-eligible professional to make MIPS program incentive payments to the professional for the year.

3. The types of healthcare professionals eligible for MIPS incentive payments may change over time. In the first and second years of the MIPS program, only physicians, physician assistants, nurse practitioners, clinical nurse specialists, and certified registered nurse anesthetists—and groups that include such professionals—will be eligible for incentive payments. The HHS Secretary will decide which other healthcare professionals, in

addition to those already specified, will be eligible in subsequent years.

B. Physician Medicare Exclusion Updates

1. New Jersey OB/GYN, agreed to be excluded from participation in Federal healthcare programs, including Medicare and Medicaid, for 20 years to settle allegations by the U.S. Department of Health and Human Services, Office of Inspector General ("OIG"), that he submitted thousands of claims for Pelvic Floor Therapy to Medicare and Medicaid for services that were either never provided or were otherwise false or fraudulent. See Labib Riachi, M.D., Department of Homeland Security News Release, New Jersey Ob/GYN Settles Fraudulent Billing Allegations, Agrees to 20-year Exclusion from Medicare, Medicaid, 2016 WL 6695917, (November 15, 2016).

2. Dr. Doron Feldman was a physician practicing as an anesthesiologist in Buffalo, New York. See Doron Feldman, M.D., (OI FILE NO. H-15-1163-9), Petitioner v The Inspector General, DAB No. CR4672, 2016 WL 4992242 (August 4, 2016). He was part of a practice called CGF Anesthesia Associates, P.C., which provided anesthesia services at various hospitals and medical facilities, including the University of Rochester-affiliated hospitals. It was alleged that Dr. Feldman conspired to defraud the University's anesthesiology department by disguising documentation to allow for payments to himself; submitting fraudulent invoices; and requesting payment for services that were never provided. In a related matter, it was alleged that Dr. Feldman filed false tax returns for the years 2008 through 2012. The administrative law judge ("ALJ") rejected Dr. Feldman's argument that his false tax returns did not involve fraudulent activities because they did not involve government programs, patient care, or drugs. The ALJ ruled that section 1128(a)(3) does not require any relationship to a government program, patient care, or drugs and applies to any felony conviction for fraud or other financial misconduct in connection with the delivery of a healthcare item or service, including management and administrative services. A 15-year exclusion period was affirmed based on one aggravating factor and no mitigating factors.

3. Petitioner and Michigan resident, Clemenceau Theophilus Acquaye, M.D., was excluded from participation in Medicare, Medicaid, and all other federal healthcare programs based on convictions for alleged criminal offenses related to the delivery of a healthcare item or service under Medicare or a state healthcare program, and the neglect or abuse of a patient in connection with the delivery of a healthcare item or service. Clemenceau Theophilus Acquaye (OI File No. 5-13-40236-9), Petitioner v The Inspector General, DAB No. CR4653, 2016 WL 4718925 (June 30, 2016). Evidence showed that Petitioner was convicted of four offenses that relate to the delivery of a healthcare item or service under the Medicaid program, including Medicaid fraud, healthcare fraud, the unlawful practice of medicine, and third degree criminal sexual conduct against a patient. A 13-year exclusion period was affirmed based on one aggravating factor and no mitigating factors.

C. Licensing Updates

1. License revocation is not excessive and harsh

Kulik v Zucker, 144 AD3d 1217 (New York November 3, 2016). In Zucker, a physician brought a review proceeding of a determination by the Hearing Committee of the State Board for Professional Medical Conduct that revoked the doctor's license to practice medicine in New York. The revocation
was based on findings that the physician intentionally misrepresented or concealed information regarding the physician's misdemeanor crime of driving while under the influence of drugs. The Supreme Court of New York affirmed the penalty of revocation of the physician's license to practice medicine. The Supreme Court based its decision on the fact that revocation was not disproportionate to the offense and that the revocation did not shock one's sense of fairness.

2. Reliable, probative, and substantial evidence

Flynn v State Med Bd of Ohio, 62 NE3d 212 (Ohio Sept 20, 2016). In a disciplinary proceeding, the appellate court affirmed the State Medical Board's decision to place a physician on probation from the practice of medicine and surgery for three years. This decision was based upon the Board's finding that the physician was impaired by mental illness. The court held that the Board could rely on findings of an examining psychiatrist in determining whether the physician was impaired by mental illness such that a restriction on the physician's license was warranted. The court also held that the Board could rely on the psychiatrist's letter even though the letter did not specifically address whether the physician had a mental illness or whether there was a causal connection between the physician's mental illness and the physician's ability to practice according to acceptable standards of care.

D. Michigan Licensing Statute Updates

1. Physician Assistants

a. Practice Agreements House Bill 5533, which amends the Public Health Code, 1978 PA 368, was adopted by both chambers of the Michigan Legislature, and signed into law by Governor Snyder in December 2016. The amendment has important implications for physician's assistants ("PAs.") House Bill 5533 updates how PAs are viewed under the law, provides greater autonomy to PAs, and describes where, when, and how PAs may practice medicine. Specifically, the bill eliminates the requirement that PAs be supervised at all times by a physician, and instead requires that PAs enter into a practice agreement with a participating physician or podiatrist. The statute states that PAs shall not engage in practice as a PA except under the terms of such a practice agreement, which meets the requirements of Section 17547. Such an agreement must include:

i. A process between the PA and participating physician for communication, availability, and decision-making when providing medical treatment to a patient;

ii. A protocol for designating an alternative physician for consultation in situations in which the participating physician is not available for consultation;

iii. The signatures of the PA and the participating physician;

iv. A termination provision that allows the PA or participating physician to terminate the PA by providing written notice at least 30 days before the date of termination;

v. The duties and responsibilities of the PA and participating physician; an

vi. A requirement that the participating physician verify the PA's credentials.

b. PA's Orders -Pursuant to the bill, a physician is not required to countersign orders written in a patient's clinical record by a PA with whom the physician has a practice agreement. Further, a physician is not required to sign an official form that lists the PA as the required signatory if that official form is signed by the PA with whom the physician has a practice agreement. See Section 17549(2). This new addition to the Public Health Code amends Section 17549, which previously required physicians to supervise PAs. This change has granted PAs substantially more autonomy than ever before.

c. Visual Screening, Testing and Postoperative Care - Pursuant to Section 17074, a PA may perform routine visual screening, testing, or postoperative care, but may not perform acts to determine the refractive state of the eye, treat refractive anomalies, or determine the spectacle or contact lens prescription to treat such anomalies. Importantly, the amendment removes any reference to requirements that the PA be supervised by a physician.

d. Rounds and House Calls - Section 17076 states that PAs may make calls or go on rounds in private homes, public institutions, emergency vehicles, ambulatory care clinics, hospitals, or other healthcare facilities in accordance with a practice agreement. Further, a PA may make calls or go on rounds as provided in this subsection without restrictions on the time or frequency of visits by a physician or the PA. Similar to 17074, the amendment removes any mention in the section of required supervision of a PA by a physician.

e. Prescribing Rights - A PA who is a party to a practice agreement may prescribe a drug in accordance with procedures and protocols for the prescription established by the department in consultation with the appropriate board. In prescribing a drug, the PA's name (and DEA registration number, if applicable) shall be used in connection with the prescription.

f. Failure To Comply - Failure to comply with the requirements results in serious disciplinary action. Section 16221 of the Public Health Code permits investigation of a licensee, registrant, or applicant for licensure or registration, and mandates that the disciplinary subcommittee shall proceed if it finds that one or more of the grounds listed in the section exists. House Bill 5533 amends Section 16221 by adding an additional ground (Section 16221(u)) by which the disciplinary subcommittee may proceed under Section 16226: failure to comply with the terms of a physician's assistant practice agreement described in section 17047(2)(a) or (b), 17547(2)(a) or (b), or 18047(2)(a) or (b).

Pursuant to the corresponding amendment of Section 16226, violation of Section 16221(u) shall result in denial, revocation, probation, suspension, limitation, reprimand, or a fine. Additionally, Section 17050 of the Public Health Code had permitted the board to prohibit a physician from supervising a PA for grounds set forth in Section 16221. It now permits the board to prohibit a physician or a PA from entering into a practice agreement. This demonstrates the new autonomy that has been granted to PAs under the amendment.

2. Maternal Death Reporting

The Public Health Code was amended at 2016 PA 479 to require a physician or an individual in charge of a health facility who was present for or was aware of a maternal death to submit information regarding the death at the time and in the manner specified by the Department of Health and Human Services for inclusion in its comprehensive health information system (HB 4235; eff. 4/6/17).

3. Midwife Licensure

The Public Health Code was amended at 2016 PA 417 to provide for the licensure of midwives (HB 4598; eff. 4/4/17).

E. False Claims Act: Escobar Upheld Implied Certification Theory

1. Background

In *Universal Health Servs, Inc v United States ex rel Escobar*, ___ US ___, 136 SCt 1989, 1995, 195 LEd2d 348 (2016), the Supreme Court rejected the contention that a government contract or regulation must expressly designate a requirement as a condition of payment in order to trigger liability under the theory of implied certification. The Court reasoned that "concerns about fair notice and open-ended liability 'can be effectively addressed through strict enforcement of the Act's materiality and scienter requirements,'" which "are rigorous." Id. at 2002. The Supreme Court held: False Claims Act liability for failing to disclose violations of legal requirements does not turn upon whether those requirements were expressly designated as conditions of payment. Defendants can be liable for violating requirements even if they were not expressly designated as conditions of payment. Conversely, even when a requirement is expressly designated a condition of payment, not every violation of such a requirement gives rise to liability. What matters is not the label the Government attaches to a requirement, but whether the defendant knowingly violated a requirement that the defendant knows is material to the Government's payment decision. Id. at 1996.

2. Implied Certification Can Be the Basis of FCA Liability

The Escobar Court also held that "the implied certification theory can be a basis for liability, at least where two conditions are satisfied: first, the claim does not merely request payment, but also makes specific representations about the goods or services provided; and second, the defendant's failure to disclose noncompliance with material statutory,

regulatory, or contractual requirements makes those representations misleading halftruths"— i.e., "representations that state the truth only so far as it goes, while omitting critical qualifying information." Id. at 2000–01 (emphasis added).

3. Materiality Standard

The Escobar court shed light on the materiality standard. The Court explained, "[a] misrepresentation about compliance with a statutory, regulatory, or contractual requirement must be material to the Government's payment decision in order to be actionable under the False Claims Act." Id. at 1996. Courts can properly dismiss a FCA claim on summary judgment based on a claimant's failure to meet the rigorous standard for materiality under the FCA. Id. at 2004 n.6. In Escobar, a unanimous Supreme Court clarified how rigorously the FCA's materiality requirement must be enforced: The materiality standard is demanding. The False Claims Act is not "an all-purpose antifraud statute" or a vehicle for punishing garden-variety breaches of contract or regulatory violations. A misrepresentation cannot be deemed material merely because the Government designates compliance with a particular statutory, regulatory, or contractual requirement as a condition of payment. Nor is it sufficient for a finding of materiality that the Government would have the option to decline to pay if it knew of the defendant's noncompliance. Materiality, in addition, cannot be found where noncompliance is minor or insubstantial. Id. at 2003 (citation omitted). The Supreme Court rejected a view that the test for materiality "is whether the person knew that the government could lawfully withhold payment." Id. at 2004 (citation omitted). The Supreme Court held that "[t]he False Claims Act does not adopt such an extraordinarily expansive view of liability," and evidence that the government "would be entitled to refuse payment were it aware of the violation" is insufficient by itself to support a finding that the violation is material to the government's payment decision. Id.

4. Government Payment Is Defense

In Escobar, the Supreme Court held that, "if the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material." Id. at 2003. "Or, if the Government regularly pays a particular type of claim in full despite actual knowledge that certain requirements were violated, and has signaled no change in position, that is strong evidence that the requirements are not material." Id. at 2003–04.

5. Escobar's Aftermath

a. Overview

With the aftermath of Escobar, the courts have been more willing to grant motions to dismiss for failing to plead the element of materiality with particularity. Similarly, to survive on summary judgment, plaintiffs must provide evidence that the alleged misrepresentations likely or actually influenced the government's decision-making process, not just that they could have done so.

b. Significant Escobar rulings

- The focus of the "government knowledge defense" changed from scienter to materiality.
- Continued payment of allegedly false claims by the government will provide a defense previously rejected by many courts.
- The definition of materiality remains vague and will cause further litigation on the meaning of this word.

III. Michigan Statutes

A. 2016 PA 359

The Public Health Code was amended to regulate the use of electronic information systems and telecommunication technologies in the delivery of healthcare (SB 753; eff. 3/29/17).

Except as otherwise provided in the amendment, a health professional shall not provide a telehealth service without directly or indirectly obtaining consent for treatment. A health professional who is providing a telehealth service may prescribe the patient a drug if both of the following are met: (a) The health professional is a prescriber; and (b) The drug is not a controlled substance.

B. 2016 PA 493

The Social Welfare Act was amended to allow disclosure of information or records that the Department of Health and Human Services possesses to the extent necessary for the proper functioning of the department or another state department (SB 1042; eff. 4/6/17).

C. 2016 PA 559

The Mental Health Code was amended to authorize the disclosure of information in the record of a recipient as necessary for the delivery of mental health services in accordance with federal privacy law (HB 5782; eff. 4/10/17).

IV. Stark Law and Anti-Kickback Updates

A. Stark Law Update: Final Rule

The Centers for Medicare and Medicaid Services ("CMS") posted a final rule on November 16,2015 ("Final Rule,") modifying the regulations implementing the federal physician self-referral law ("Stark Law.") These new regulatory provisions became effective on January 1, 2016, with the exceptions of a few clarifying changes of existing policy, and the amended definition of "ownership or investment interest," which were effective January 1, 2017. Some significant physicians provisions are:

1. Assistance to compensate a non-physician practitioner

This exception allows remuneration from a hospital, federally-qualified health center, or rural health clinic to a physician to recruit a NPP, where substantially all (i.e., 75%) of the services furnished by the NPP to the patients of the physician's practice are for primary care services or mental healthcare services. This exception applies to the following NPPs: (1) physician assistants; (2) nurse practitioners; (3) clinical nurse specialists; (4) certified nurse midwives; (5) clinical social workers; and (6) clinical psychologists. See, 42 CFR 411.357(x).

2. Clarification on the writing requirement

The Final Rule removes the term "agreement" from most exceptions and clarifies the requirement that an arrangement be in writing. A single "formal contract" is not required. The following may satisfy the contract requirement: (a) collection of documents may satisfy the writing requirement; (b) collection of documents may include "contemporaneous documents evidencing the course of conduct between the parties." See 80 FR 71315. "[T]he relevant inquiry is whether the available contemporaneous documents (that is, documents that are contemporaneous with the arrangement) would permit a reasonable person to verify compliance with the applicable exception at the time that a referral is made." 80 FR 71315.

3. Clarification on the 1-year term requirement for office space rental, equipment rental, and personal service arrangements

The Final Rule clarifies that the arrangement itself must have a duration of at least one year, but a formal "term" provision in a contract is not required. Instead, the duration requirement can be shown through contemporaneous documents establishing the arrangement lasted for at least one year. However, if the arrangement was terminated during the first year, the parties must be able to show they did not enter into a new arrangement for the same space, equipment, or services during the first year. See, 42 CFR 411.357(a), 42 CFR 411.357(b), 42 CFR 411.357(d).

4. "Temporary noncompliance with signature" requirement

Changes it to a blanket 90-day period to comply with this requirement, regardless of whether the failure to obtain a signature was inadvertent or not. See, 42 CFR 411.353(g).

5. Holdover arrangements

The Final Rule provides for an indefinite holdover provision in the Rental of Office Space Exception, Rental of Equipment Exception, and Personal Services Exception. CMS also finalized its proposal to amend the Fair Market Value Compensation Exception to allow arrangements of any time frame to be renewed for any number of times (as long as the arrangement continues to comply with the other requirements of the exception, rather than just renewals of arrangements made for less than one year. See, 42 CFR 411.357(l)

6. Stand in the shoes

The Final Rule clarifies that a physician who is standing in the shoes of his or her physician organization has satisfied the signature requirement of an applicable exception when the authorized signatory of the physician organization has signed the writing. For purposes other than the signature requirement, all physicians in a physician organization are considered to be "parties" to the compensation arrangement. See, 42 CFR 411.354(c)(3)(i).

7. Timeshare Arrangements Exception

This exception covers "use" arrangements only, which includes the use of premises, equipment (excluding advanced imaging equipment, radiation therapy equipment, and (most) clinical or pathology laboratory equipment), personnel, items, supplies, or services. Traditional office space leases and arrangements conveying a possessory leasehold interest in office space are not covered under this exception. Compensation for such arrangements must be carefully structured, as percentage compensation and per-unit services fees (i.e., "per-use" and "per-patient" rates) are prohibited but hourly or half day rates are acceptable. 42 CFR 411.357(y).

B. Anti-Kickback Law Updates

On December 7, 2016, the OIG published a final rule to amend the Anti-Kickback Statute ("AKS") by adding new safe harbors ("Final Rule"). The Final Rule also revises the definition of "remuneration" in the civil monetary penalty ("CMP") rule. The Final Rule became effective on January 6, 2017. See, 81 Fed. Reg. 88368 (December 7, 2016). The Final Rule will more than likely be of most significance to hospitals, pharmacies, and public ambulance services. Manufacturers are explicitly excluded from utilizing many of the new and revised protections under the Final Rule. The safe harbor regulations are found at 42 CFR 1001.952. Significant physicians provisions are:

1. New and revised safe harbor for waiver of beneficiary copayment, coinsurance and deductible amounts

Expands the scope of the safe harbor for cost-sharing waivers offered by healthcare providers, to include all federal healthcare programs. The safe harbor previously applied only to Medicare and state healthcare program beneficiaries. The Final Rule also revises the definition of cost-sharing to include coinsurance in addition to copayment and deductibles. The changes will potentially allow healthcare providers (but not manufacturers) to offer these cost-saving programs to a larger segment of their patient population.

2. Technical correction to the safe harbor for referral services

The Final Rule makes a technical correction to the safe harbor for referral services. It states remuneration paid to the referral source must not be based on the volume or value of any

referrals, to or "business otherwise generated by[,] either party for the other party." See, 42 CFR 1001.952(f) (emphasis added).

3. New local transportation services safe harbor for "Established Patients."

The Final Rule creates a safe harbor protecting free or discounted local transportation services provided by a healthcare provider or supplier to federal healthcare program beneficiaries to receive medically- necessary items or services. This safe harbor as to free or discounted local transportation does not apply to healthcare providers that primarily supply healthcare items (i.e., pharmacies, durable medical equipment suppliers, and pharmaceutical and device manufacturers). The safe harbor generally applies to transportation services within 25 miles of the healthcare provider or supplier (50 miles if the patient resides in a rural area) that are not marketed or advertised.

C. Revisions to Civil Monetary Penalty Rules

1. Remuneration

The Final Rule also revises the definition of "remuneration" under the CMP rules. The CMP prohibits the offer or transfer of remuneration to Medicare and state healthcare program beneficiaries to influence those beneficiaries to obtain reimbursable services from a particular provider, practitioner, or supplier. "Remuneration" under the CMP rules now includes coinsurance, in addition to copayment and deductible amounts, and is consistent with the definition of remuneration under the CMP statute. See, 42 CFR 1003.110.

2. Nominal Value

In addition to the exceptions highlighted above, the Final Rule adjusts OIG's interpretation of nominal value under the CMP statute to mean $15 for an individual gift and $75 in the aggregate annually per patient, which are increases from the prior definitions of $10 per instance and $50 per year. See, Department of Health and Human Services, Office of Inspector General, Office of Inspector General Policy Statement Regarding Gifts of Nominal Value to Medicare and Medicaid Beneficiaries, December 7, 2016. https://oig.hhs.gov/fraud/docs/alertsandbulletins/OIG-Policy-Statement-Giftsof-Nominal-Value.pdf.

V. Phase 2 HIPAA Audits

A. OCR HIPAA Phase 2 Audit Info can be found

- http://www.hhs.gov/hipaa
- Twitter @hhsocr
- http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

• Sign Up for the OCR Privacy Listserv—OCR has established a listserv to inform the public about Privacy and Security Rule FAQs, guidance, and technical assistance materials as they are released.

1. Three (3) Rounds in HIPAA Phase 2 Audits

HIPAA Phase 2 audits are being conducted by OCR staff and a contractor and funded in part from assessed penalties. Phase II has been designed to:

- Examine mechanisms for compliance
- Identify industry best practices
- Discover risks and vulnerabilities not surfaced through enforcement activities
- Enable OCR to get out in front of problems before they result in breaches

a. To create a diverse pool of potential audit eligible candidates, OCR sent emails to covered entities and business associates to verify their contact information followed by a questionnaire.

- All covered entities and business associates are eligible for an audit. Two hundred Phase 2 audits (in total) are expected.
- OCR ran a randomized selection algorithm that drew from covered entity types, (e.g., health care provider, health plan, clearinghouse, business associate), size, public or private and location and resulted in 167 covered entities.
- OCR notified those selected for an audit by email in a "document request letter." The letter specified the documents to be provided, introduced the audit team, explained the audit process, and set expectations.
- OCR expects auditees to give auditors their full cooperation and support.

b. Round 1 began in the summer—OCR sent emails initiating desk audits to 167 covered entities on July 11, 2016.

2. Round 2. Lists of business associates will be used to select business associates for round two of the Phase 2 audits.

a. Audits of BAs are expected to focus on breaches and security.

3. Phase 2 Round 3 in 2017: The third round of the Phase 2 audits involves up to 50 more comprehensive onsite audits of both covered entities and business associates, bringing the total number of Phase 2 audits to between 200 and 250.

Audits are primarily a compliance improvement activity to help OCR to

- better understand compliance efforts with particular aspects of the HIPAA Rules
- determine what types of technical assistance OCR should develop
- develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches

Questions and Answers: OCR has provided FAQs for entities selected for desk audits. The FAQs also are reviewed in webinars and posted on the OCR website. They address

technical, administrative and general questions. The guidance will assist entities being audited and provides insights regarding OCR's expectations for those not currently being audited.

B. Threats and Breaches

1. Most common data breach is an unauthorized access or disclosure of PHI. Data breaches include improper actions by those inside the organization, as well as external attacks including phishing, hacking, and ransomware.

a. Both CMS and the OCR take the position that a ransomware attack also is a data breach which must be reported like any HIPAA violation, and a ransomware attack is a reportable security incident and must be publicly reported in a timely manner or a covered entity or business associate will face severe penalties.

b. Employees disclosing information—Employees' gossiping about patients to friends or coworkers is also a HIPAA violation that can cost a practice a significant fine.

c. Medical records mishandling—Another very common HIPAA violation is the mishandling of patient records. If a practice uses written patient charts or records, they must be kept locked away and safe out of the public's view.

d. Lost or Stolen Devices—Theft of PHI (protected health information) through lost or stolen laptops, desktops, smartphones, and other devices that contain patient information can result in HIPAA fines. Mobile devices are the most vulnerable to theft because of their size; therefore, the necessary safeguards should be put into place such as password protected authorization and encryption to access patient-specific information.

e. Texting patient information—Texting patient information such as vital signs or test results is often an easy way that providers can relay information quickly. It is potentially placing patient data in the hands of cyber criminals who could easily access this information. There are new encryption programs that allow confidential information to be safely texted, but both parties must have it installed on their wireless device, which is typically not the case.

f. Social Media—Posting patient photos on social media is a HIPAA violation. Make sure all employees are aware that the use ofsocial media to share patient information is considered a violation of HIPAA law.

g. Employees illegally accessing patient files—Employees accessing patient information when they arenot authorized is another very common HIPAA violation. Whether it is out of curiosity, spite, or as a favor for a relative or friend, this is illegal and can cost a practice substantially. Also, individuals that use or sell PHI for personal gain can be subject to fines and even prison time.

h. Social breaches—An accidental breach of patient information in a social situation is quite common, especially in smaller more rural areas.

i. Authorization Requirements—A written consent is required for the use or disclosure of any individual's personal health information that is not used for treatment, payment, healthcare operations, or permitted by the Privacy Rule. If an employee is not sure, it is always best to get prior authorization before releasing any information.

j. Accessing patient information on home computers—Most clinicians use their home computers or laptops after hours from time to time to access patient information to record notes or follow-ups. This could potentially result in a HIPAA violation if the screen is accidentally left on and a family member uses the computer. Make sure your computer and laptop are password protected and keep all mobile devices out of sight to reduce the risk of patient information being accessed or stolen.

k. Lack of training—One of the most common reasons for a HIPAA violation is an employee who is not familiar with HIPAA regulations. Often only managers, administration, and medical staff receive training although HIPAA law requires all employees, volunteers, interns and anyone with access to patient information to be trained. Compliance training is one of the most proactive and easiest ways to avoid a violation.

C. Breach Reporting and Investigations

1. HIPAA covered entities are obligated to report breaches to the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services. Initially OCR investigated larger breaches (affecting over 500 individuals). In August 2016, OCR announced that its Regional Offices will expand initiatives to investigate smaller breaches.

a. OCR will investigate breaches occurring at covered entities or at business associates, even though only covered entities have a direct obligation to report to OCR. The Regional Offices will have discretion to decide which smaller breaches to investigate, taking into account factors such as the following:

1. The size of the breach;
2. Theft of or improper disposal of unencrypted PHI;
3. Breaches that involve unwanted intrusions to IT systems (for example, by hacking);
4. The amount, nature and sensitivity of the PHI involved; or
5. Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

b. OCR has stated that even covered entities that habitually report statistically few breaches will now be on its radar screen. If that reporting pattern is below the norm for comparable entities, OCR's suspicion may be raised about the non-reporting entity's ability to recognize and remediate breach events. Under the Breach Notification Rule, all improper disclosures of or access to unsecured protected health information are presumed

to be a reportable breach, unless the covered entity can affirmatively demonstrate that there is only a low risk that the protected health information has been compromised—all as defined in the rule.

c. This all means that HIPAA covered entities need to take their breach reporting responsibilities even more seriously than before. It also means that HIPAA covered entities and business associates must enhance their focus on the safeguards that can prevent a breach, detect one when it does occur, and respond immediately to remediate and mitigate its effects. These safeguards range from highly sophisticated cyber technology applications to very low tech precautions relating to human behavior.

D. Enforcement

1. The compliance issues investigated most are, compiled cumulatively, in order of frequency:

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Lack of administrative safeguards of electronic protected health information; and
- Use or disclosure of more than the minimum necessary protected health information.

2. The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:
- Private Practices;
- General Hospitals;
- Outpatient Facilities;
- Pharmacies; and
- Health Plans (group health plans and health insurance issuers).

OCR advises that they focus enforcement on cases that identify industry-wide noncompliance where corrective action may be the only remedy and where corrective action benefits the greatest number of individuals.

Statistics

Since the compliance date of the Privacy Rule in April 2003:

- OCR has received over 144,662 HIPAA complaints. We have resolved ninety-seven percent of these cases (141,235).
- OCR has investigated and resolved over 24,617 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates. Corrective actions obtained by OCR from these entities have resulted in change that is systemic and that affects all the individuals they serve. OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates

noncompliance by the covered entity or their business associate, which may include settling with the entity in lieu of imposing a civil money penalty.

- To date, OCR has settled 41 such cases resulting in a total dollar amount of $48,679,700.00.
- OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.
- In another 11,124 cases, our investigations found no violation had occurred.
- Additionally, in 17,176 cases, OCR has intervened early and provided technical assistance to HIPAA covered entities, their business associates, and individuals exercising their rights under the Privacy Rule, without the need for an investigation.
- In the rest of our completed cases, (88,318) OCR determined that the complaint did not present an eligible case for enforcement. These include cases in which:

• OCR lacks jurisdiction under HIPAA. For example, in cases alleging a violation by an entity not covered by HIPAA;
• The complaint is untimely, or withdrawn by the filer. The activity described does not violate the HIPAA Rules;
• The activity described does not violate the HIPAA Rules. For example, in cases where the covered entity has disclosed protected health information in circumstances in which the Privacy Rule permits such a disclosure.

In its news releases announcing settlements OCR is highlighting lessons to be learned. Among the takeaways are
• ePHI Safeguards
• Managing Business Associates
• Timely breach notification
• Assessing and Managing Security Risks
• Malware prevention
• Managing Disclosures

OCR has stated it hopes resolution agreements will provide a template for other health care entities to take proactive steps to ensure HIPAA compliance.

- HIPAA settlement demonstrates importance of implementing safeguards for ePHI—January 18, 2017
- First HIPAA enforcement action for lack of timely breach notification settles for $475,000—January 9, 2017
- UMass settles potential HIPAA violations following malware infection—November 22, 2016
- $2.14 million HIPAA settlement underscores importance of managing security risk—October 17, 2016
- HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements—September 23, 2016
- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million—August 4, 2016

- Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)—July 21, 2016
- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University—July 18, 2016
- Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement—June 29, 2016
- Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital—April 21, 2016
- $750,000 settlement highlights the need for HIPAA business associate agreements—April 19, 2016
- Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement—March 17, 2016
- $1.55 million settlement underscores the importance of executing HIPAA business associate agreements—March 16, 2016
- Physical therapy provider settles violations that it impermissibly disclosed patient information—02/16/2016

1. New Administration

a. First, there is a recognition of the relatively weak state of the country's cybersecurity efforts. While it is unlikely that we will see new regulations affecting security issues (as discussed below), the issue of cyber-readiness will be one to watch frequently.

b. Second, there is a willingness in the new Administration to engage in broad surveillance of individuals in connection with national security activities. More companies will be faced with the need to deal with data demands from the government that place the company in direct conflict with its customers and/or employees. The impact of these surveillance issues may be felt most broadly in connection with international privacy regulation, where the more aggressive the United States is in connection with surveillance, the less flexible we may find the European authorities and others in connection with international data flows.

c. Third, expect less government regulation and expenditure of less government money. This likely means no new regulations and somewhat less enforcement, rather than broader changes and a rollback
on existing privacy rights.

2. Government Privacy and Security Leadership

a. The key issue will be the senior leadership of the key privacy enforcement agencies—including the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights, the Federal Communications Commission (FCC) and others—as well as the fate of the primary "day to day" senior staff who constitute the bulk of the thought leadership and institutional memory of these offices.

b. For HHS (which oversees the HIPAA Rules), we can expect to see a new director of the Office for Civil Rights (OCR), with a likely "interim" leader" as well. We likely

will see new leadership in most key privacy positions (although not immediately), and a resulting likelihood of somewhat less enforcement and perhaps some pushback on existing regulatory compliance obligations.

The purpose of these seminar materials is to present information on the topics presented. The brevity of this document prevents comprehensive treatment of all legal issues, and the information contained herein should not be taken as legal advice. Because of the changing nature of employment law, and these areas in particular, legal counsel should be consulted before any particular action is undertaken or a decision is made that may lead to a challenge or a lawsuit of these laws. Advice for specific matters should be sought directly from legal counsel.