BRACH | EICHLER LLC

Health Law UPDATE

May 2019

In This Issue:

FEDERAL UPDATE

2020 CMS Call Letter and Policy Changes

Centers for Medicare & Medicaid Services (CMS) released, on April 1, 2019, its conclusions in response to the public's comments to CMS's proposed changes to Medicare Advantage (MA) and Part D programs. The initial request for the public's feedback was to assist CMS in its commitment to enhancing the options and flexibility for Medicare beneficiaries. CMS is striving to make the system easier to use and allow for further innovation.

As a result of the comments received, by 2020 CMS will implement the alternative payment condition count (APCC) model, which will provide a blended risk score calculation. Per the 21st Century Cures Act, CMS is required to adjust the risk adjustment model to account for the number of conditions an individual may have and to continue to adjust for future conditions. This risk adjustment model is required to be fully implemented by 2020. CMS has begun to phase in the new model and, as of 2019, CMS will calculate risk using a 50/50 split of the 2017 accounting model and the new APCC model, which will account for such conditions as pressure ulcers and dementia.

As CMS phases in the new risk adjustment model, it is also phasing in a new model to calculate risk scores. In previous years, CMS has calculated risk scores using diagnosis information submitted into the Risk Adjustment Processing System (RAPS) and from Medicare Fee for Services (FFS). Currently, CMS has begun collecting data from MA encounter data. By 2020, CMS will blend the risk score 50/50 between encounter data and diagnosis information submitted through RAPS.

Another policy change for 2020 will be a 5.9% coding pattern adjustment. By law, CMS is required to adjust plan payments to reflect changes in diagnosis coding between MA and FFS providers. CMS is also finalizing the updates regarding how MA and Part D sponsors will be paid.

In the CMS 2020 Final Call Letter, CMS addresses the opioid crisis and CMS's continued commitment to find solutions. CMS notes that, in certain circumstances, opioid medications may be necessary but encourages organizations to reevaluate their current policies regarding coverage and utilization to determine if a multimodal pain care plan is being used. CMS is finalizing polices for 2020 to assist Medicare plan sponsors in combatting this crisis. CMS policies include access to opioid reversal agents, Star Ratings, and partnering with plans to utilize alternative and integrative treatment plans for individuals with chronic pain and those who suffer from addiction.

For more information, contact:

Joseph M. Gorrell | 973.403.3112 | jgorrell@bracheichler.com
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com
Erika Marshall | 973.364.5236 | emarshall@bracheichler.com

DOJ: Massive Telemedicine and DME Fraud Scheme Uncovered

On April 1, 2019, the U.S. Department of Justice (DOJ) published an announcement regarding federal indictments and law enforcement actions involving telemedicine and durable medical equipment (DME) marketing executives, resulting in charges against 24 individuals responsible for over $1.2 billion in losses. The scheme was investigated by the FBI and the U.S. Department of Health & Human Services, Office of Inspector General (OIG) and prosecuted by the DOJ. The defendants in the prosecution included CEOs, COOs, and others associated with five telemedicine companies, the owners of dozens of DME companies, and three licensed medical professionals. In addition to the DOJ prosecution, the Centers for Medicare & Medicaid Services (CMS) Center for Program Integrity (CMS/CPI) took adverse administrative action against 130 DME companies that had submitted over $1.7 billion in claims and received over $900 million in payments.

According to the DOJ's announcement:

> "The charges announced today target an alleged scheme involving the payment of illegal kickbacks and bribes by DME companies in exchange for the referral of Medicare beneficiaries by medical professionals working with fraudulent telemedicine companies for back, shoulder, wrist and knee braces that are medically unnecessary. Some of the defendants allegedly controlled an international telemarketing network that lured over hundreds of thousands of elderly and/or disabled patients into a criminal scheme that crossed borders, involving call centers in the Philippines and throughout Latin America. The defendants allegedly paid doctors to prescribe DME either without any patient interaction or with only a brief telephonic conversation with patients they had never met or seen. The proceeds of the fraudulent scheme were allegedly laundered through international shell corporations and used to purchase exotic automobiles, yachts and luxury real estate in the United States and abroad."

The DOJ stated that:

> "According to allegations in court documents, some of the defendants obtained patients for the scheme by using an international call center that advertised to Medicare beneficiaries and "up-sold" the beneficiaries to get them to accept numerous "free or low-cost" DME braces, regardless of medical necessity. The international call center allegedly paid illegal kickbacks and bribes to telemedicine companies to obtain DME orders for these Medicare beneficiaries. The telemedicine companies then allegedly paid physicians to write medically unnecessary DME orders. Finally, the international call center sold the DME orders that it obtained from the telemedicine companies to DME companies, which fraudulently billed Medicare. Collectively, the CEOs, COOs, executives, business owners and medical professionals involved in the conspiracy are accused of causing over $1 billion in loss."

For more information, contact:

Riza I. Dagli | 973.403.3103 | rdagli@bracheichler.com
Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
John D. Fanburg | 973.403.3107 | jfanburg@bracheichler.com

Privacy Concerns Associated with Cameras in Hospitals

Eighty-one women are suing a California hospital alleging, among other things, that the hospital violated their privacy rights by filming them during medical procedures. The claims in the lawsuit include breach of fiduciary duty, invasion of privacy-intrusion into private affairs, invasion of privacy under California law, negligence, negligent infliction of emotional distress, and unlawful recording of confidential information in violation of California law.

The plaintiffs in the lawsuit allege that, during a period of time in 2012 and 2013, the hospital secretly operated hidden motion-detecting cameras in the hospital's labor and delivery rooms. According to the complaint filed in the action, the cameras recorded video images of births, including C-sections; birth complications; dilation and curettage to resolve miscarriages; hysterectomies; sterilizations; and other medical procedures. According to the complaint, over 18,000 patients were recorded. The plaintiffs allege that the hospital was negligent in maintaining the records, which were stored on desktop computers and were easily accessible by multiple users, some without password protections, and that the hospital did not log or track employees accessing the recordings. According to the complaint, the hospital claimed that the hidden camera surveillance was intended to address employee theft of Propofol from drug carts in the operating room.

The case should serve as a warning and reminder to hospitals and other healthcare providers about patients' reasonable expectations of privacy, and the myriad of privacy laws aimed at protecting sensitive health information, including images of patients.

For more information, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com
Cynthia J. Liba | 973.403.3106 | cliba@bracheichler.com

Extension of Comment Period: Proposed Rules to Improve Interoperability of EHR Information

In response to requests from a variety of stakeholders, on April 19, 2019, the U.S. Department of Health & Human Services (DHHS) published an announcement about its extension of the public comment period for two proposed regulations concerning the interoperability of health information technology, or "health IT" and enabling patients to electronically access their health information. The new deadline for submission of comments is June 3, 2019. By way of background:

> On February 11, 2019, HHS announced two proposed rules to support the seamless and secure access, exchange, and use of electronic health information (with *Federal Register* publication on March 4, 2019). The rules would increase choice and competition while fostering innovation that promotes patient electronic access to and control over their health information. Together the proposed rules address both technical and healthcare industry factors that create barriers to the interoperability of health information and limit a patient's ability to access essential health information. Addressing those challenges will help to drive an interoperable health IT infrastructure across systems, enabling healthcare providers and patients to have access to health data when and where it is needed.

DHHS provided the following links to related information:

ONC proposed rule

Trusted Exchange Framework and Common Agreement and the Notice of Funding Opportunity

CMS Interoperability Efforts Listserv

CMS Proposed Rule Fact Sheet (CMS-9115-P)

CMS Proposed Rule (CMS-9115-P)

OCR FAQ

For more information, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com
John D. Fanburg | 973.403.3107 | jfanburg@bracheichler.com
Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com

STATE UPDATE

New Jersey Legislative Update

Bundled Payments for Childbirth-Related Services Approved by NJ Legislature – On March 25, 2019, the New Jersey Senate and the New Jersey Assembly passed Bill S3365, which would establish bundled payments for childbirth-related services. The Bill now awaits Governor Murphy's signature. The Bill will implement a three-year Medicaid perinatal episode of care pilot program, to be developed by the "perinatal episode of care steering committee" established under the Bill. The steering committee will design a perinatal episode of care payment model, also known as a bundled payment model, in which provider reimbursement will be based on target total cost of care for services provided within a perinatal episode of care, rather than on individual services provided within the episode of care. The Bill defines a "perinatal episode of care" as all pregnancy-related care including prenatal care, labor and birth, and postpartum care provided to a mother and infant, beginning 40 weeks prior to the delivery and ending 60 days after the delivery of the infant. The purpose of the Bill is to improve perinatal healthcare outcomes and to reduce the cost of perinatal care.

New Law to Enhance Enforcement and Oversight of Behavioral Health Parity Laws – On April 11, 2019, Bill A2031 was signed into law by Governor Murphy to enhance enforcement and oversight of behavioral health parity laws. The new Law requires hospitals, medical and health service corporations, commercial insurers, health maintenance organizations, health benefits plans issued pursuant to the New Jersey Individual Health Coverage and Small Employer Health Benefits Programs, the State Health Benefits Program, and the School Employees' Health Benefits Program, to provide coverage for mental health conditions and substance-use disorders to meet the requirements of the federal Paul Wellstone and Pete Domenici Mental Health Parity and Addiction Equity Act of 2008. That act prevents certain health insurers that provide mental health or substance-use disorder benefits from imposing less favorable benefit limitations on those benefits than on medical or surgical benefits, commonly referred to as mental health parity. The new Law amends several statutes which require hospitals, medical and health service corporations, individual and group health insurers, and the State Health Benefits Program to provide coverage for biologically based mental illness under the same terms and conditions as provided for any other sickness. The new Law expands that coverage to include mental health conditions and substance-use disorders.

Bill Establishing Maternal Health Care Pilot Program Approved by New Jersey Legislature – On March 25, 2019, the New Jersey Senate and the New Jersey Assembly passed Bill S3375, which would require

the Commissioner of Health to develop a shared decision-making tool for use by maternity care hospitals and licensed birthing centers. The Bill now awaits Governor Murphy's signature. Use of the shared decision-making tool by maternity care hospitals and licensed birthing centers would be voluntary. The purpose of the tool would be to: improve knowledge of the benefits and risks of, and best practice standards for, the provision of maternity care; increase collaboration between a maternity care patient and the patient's health care provider to assist the patient in making informed decisions about the maternity care the patient receives; improve patient experiences during, and reduce adverse outcomes related to, or associated with, pregnancy; and encourage maternity care patients to create a birth plan which would provide the patient's preferences during the stages of labor, delivery, and postpartum. The Bill directs the Commissioner of Health to implement a three-year pilot program, under which a select number of maternity care hospitals and birthing centers will utilize and evaluate the shared decision-making tool.

For more information, contact:

Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
John D. Fanburg | 973.403.3107 | jfanburg@bracheichler.com
Ed Hilzenrath | 973.403.3114 | ehilzenrath@bracheichler.com

Brach Eichler In The News

John D. Fanburg and Joseph Gorrell participated in a panel discussion at the New Jersey Institute for Continuing Legal Education on April 17. The session was entitled "Effectively Representing Physicians: Everything You Need to Know to Successfully Represent New Jersey Physicians in 2019."

Lani M. Dornfeld will address attendees at the Home Care and Hospice Association of New Jersey Annual Meeting, June 6, on "HIPAA Breach Response, Investigation and Reporting: How to Follow the Rules to Reduce Fines and Penalties (and What the Rules Don't Say, But You Need to Know)."

Register Now! Our tenth annual New Jersey Healthcare Market Review (NJHMR) will be held on September 18 - September 19 at the Borgata in Atlantic City.

To view a full listing of recent news items and to read the articles mentioned above, please click here.

HIPAA CORNER

OCR's Warnings Regarding Advanced Persistent Threats and Zero Day Vulnerabilities

The OCR warns, in its Spring 2019 Cybersecurity Newsletter, that advanced persistent threats (APT) and "zero day" exploits are dangerous enough independently, but when used in combination, they are a truly disastrous combination. APTs and zero day threats already have been implicated in several cyberattacks on the healthcare sector in the U.S. and around the world.

An APT is a long-term cybersecurity attack that continuously attempts to find and exploit vulnerabilities in a target's information systems to steal information or disrupt the target's operations. Although individual APT attacks need not be technologically sophisticated, the persistent nature of the attack, as well as the attacker's ability to change tactics to avoid detection, make APTs a formidable threat to any information technology system (especially to those that are part of the healthcare field). APTs can compromise the security of protected health information (PHI), making it vulnerable to identity theft. Any security incident impacting the confidentiality, integrity, or availability of PHI can directly affect the health and safety of citizens.

One of the most dangerous tools in a hacker's arsenal is the zero day attack which takes advantage of a previously unknown hardware, firmware, or software vulnerability. Zero day attacks are especially dangerous because their novel nature makes them more difficult to detect and contain than standard hacking attacks. The possibility of such an attack emphasizes the importance of an organization's overall security management process which includes monitoring of anti-virus or cybersecurity software for detection of suspicious files or activity. Zero day exploits make it possible for hackers to gain unauthorized access to an organization's computer system and PHI.

An APT using a zero day exploit is a recipe for disaster which can threaten computers and data all over the world. One such example is the EternalBlue exploit and the WannaCry ransomware. EternalBlue targeted vulnerabilities in several of Microsoft's Windows operating systems and then WannaCry infected hundreds of thousands of computers around the world, including several HIPAA-covered entities and business associates in the United States. The damages due to this cyberattack are estimated to be in the billions of dollars.

The OCR recommends that organizations proactively implement the HIPAA Security Rule's required security measures which can help in preventing, detecting, and responding to cyberattacks from APTs and zero day exploits, as follows:

- Conducting risk analyses to identify risks and vulnerabilities
- Implementing a risk management process to mitigate identified risks and vulnerabilities
- Regularly reviewing audit and system activity logs to identify abnormal or suspicious activity
- Implementing procedures to identify and respond to security incidents
- Establishing and periodically testing contingency plans including data backup and disaster recovery plans to ensure data is backed up and recoverable
- Implementing access controls to limit access to ePHI
- Encrypting ePHI, as appropriate, for data-at-rest and data-in-motion
- Implementing a security awareness and training program, including periodic security reminders and education and awareness of implemented procedures concerning malicious software protection, for all workforce members.

Cyber security guidance material is also available on the U.S. Department of Health & Human Services webpage.

HHS Issues "Enforcement Discretion" Notice Concerning HIPAA Penalties

On April 30, 2019, the U.S. Department of Health & Human Services (HHS) issued a Notice of Enforcement Discretion in the Federal Register (Notice) to inform the public about how it applies HHS regulations concerning the assessment of civil monetary penalties (CMPs) for HIPAA violations.

Both civil and criminal penalties are possible under HIPAA. Civil monetary penalties are tiered across four categories based on the violation type: (1) the person did not know (and, by exercising reasonable diligence, would not have known) that the person violated the provision of HIPAA at issue, (2) the violation was due to reasonable cause, and not willful neglect, (3) the violation was due to willful neglect that is timely corrected, and (4) the violation was due to willful neglect that is not timely corrected. In publishing the HIPAA Enforcement

Rule in 2013, HHS interpreted HIPAA's statutory language to apply civil monetary penalties in the following manner:

Culpability	Min. Penalty/ Violation	Max. Penalty/ Violation	Annual Limit Identical Violations
No Knowledge	$100	$50,000	$1,500,000
Reasonable Cause	$1,000	$50,000	$1,500,000
Willful Neglect – Corrected	$10,000	$50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$50,000	$1,500,000

The fourth column indicates the annual limit for all violations of an identical requirement or prohibition. In commentary to the 2013 HIPAA Enforcement Rule, HHS noted that some commenters expressed concern about the $1.5 million cap for every penalty tier, and that this was inconsistent with the HITECH Act. At the time, HHS stated that it continued to believe the penalty amounts were appropriate and reflected "the most logical reading of the HITECH Act."

In the Notice, HHS stated that, upon further review, "the better reading" of the HITECH Act is to apply the annual limits as follows:

Culpability	Min. Penalty/ Violation	Max. Penalty/ Violation	Annual Limit Identical Violations
No Knowledge	$100	$50,000	$25,000
Reasonable Cause	$1,000	$50,000	$100,000
Willful Neglect – Corrected	$10,000	$50,000	$250,000
Willful Neglect – Not Corrected	$50,000	$50,000	$1,500,000

HHS advised that it will use the above civil money penalty structure, as adjusted for inflation, effective as of the date of the Notice and until further notice. HHS also commented that it "expects to engage in future rulemaking to revise the penalty tiers in the current regulation to better reflect the text of the HITECH Act."

It will be interesting to watch HHS's implementation of the revised annual limit interpretation and whether some of the shocking penalties of the past couple years will continue to be seen, e.g., a $5.5 million penalty assessed against Memorial Healthcare System in 2017 and a $16 million penalty assessed against Anthem in 2018. Perhaps HHS will issue more violations in each case it reviews to make up the difference. Perhaps HHS will issue more lower-end penalties in lieu of its determination to provide "technical assistance" rather than a penalty in certain cases.

For now, we will have to wait and see whether covered entities and business associates will benefit from the HHS's updated interpretation of the tiered penalty structure. What we do know for sure is that willfully neglectful behavior will result in maximum penalties. This type of behavior may include not having up-to-date policies in place, not having business associate agreements in place where needed, and not performing periodic risk analyses and addressing identified risks and vulnerabilities.

If you need assistance in managing a breach incident or making any required reporting, please contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

BRACH | EICHLER LLC

bracheichler.com | Counsellors at Law

Health Care Practice Group | 101 Eisenhower Parkway, Roseland, NJ 07068 | 973.228.5700

Members

Riza I. Dagli | 973.403.3103 | rdagli@bracheichler.com
Lani M. Dornfeld, HLU Editor | 973.403.3136 | ldornfeld@bracheichler.com
John D. Fanburg, Chair | 973.403.3107 | jfanburg@bracheichler.com
Joseph M. Gorrell | 973.403.3112 | jgorrell@bracheichler.com
Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com

Counsel

Shannon Carroll | 973.403.3126 | scarroll@bracheichler.com
Lauren D. Goldberg | 973.364.5228 | lgoldberg@bracheichler.com
Debra W. Levine | 973.403.3142 | dlevine@bracheichler.com
Randall H. Lee | 973.364.5205 | rlee@bracheichler.com
Richard B. Robins | 973.403.3147 | rrobins@bracheichler.com
Jonathan J. Walzman | 973.403.3120 | jwalzman@bracheichler.com
Edward J. Yun | 973.364.5229 | eyun@bracheichler.com

Associates

Colleen Buontempo | 973.364.5210 | cbuontempo@bracheichler.com
Lindsay P. Cambron | 973.364.5232 | lcambron@bracheichler.com
Jocelyn Ezratty | 973.364.5211 | jezratty@bracheichler.com
Susan E. Frankel | 973.364.5209 | sfrankel@bracheichler.com
Ed Hilzenrath | 973.403.3114 | ehilzenrath@bracheichler.com
Cynthia J. Liba | 973.403.3106 | cliba@bracheichler.com
Erika Marshall | 973.364.5236 | emarshall@bracheichler.com

Stay Connected!

*Follow us on **LinkedIn**: www.linkedin.com/company/brach-eichler-llc and **Twitter**: http://twitter.com/BrachEichler*

You have the option of receiving your **Health Law Updates** *via e-mail if you prefer, or you may continue to receive them in hard copy. If you would like to receive them electronically, please provide your e-mail address to adejesus@bracheichler.com. Thank you.*