Vital Sounds
A Newsletter for Health Care Professionals and Facilities
KaMMCO
Kansas Medical Mutual Insurance Company
www.KaMMCO.com

Physician-led KaMMCO Admitted to Connecticut Insurance Market

KaMMCO is pleased to announce the company has been admitted to sell medical professional liability insurance and cyber security insurance in the State of Connecticut. KaMMCO enters the Connecticut market with support from the Connecticut State Medical Society.

"We are proud to work with the Connecticut State Medical Society to grow our insurance business," said Kurt Scott, president and chief executive officer of KaMMCO. "We are honored they recognize us as their medical professional liability insurance *Preferred Affinity Partner*."

KaMMCO began the licensing process early 2017 and received notification from the Connecticut Insurance Department on February 23. "In working closely with the Connecticut State Medical Society on the development and launch of CTHealthLink, the physician-led health information exchange, it became clear that there was an opportunity to further serve the physicians and healthcare providers of Connecticut with valuable insurance products," Scott added.

KaMMCO will be working with the organization's brokerage firm, CSMS Insurance Agency, and anticipates quoting coverage later this spring.

KaMMCO Spring Education Series Presents March Webinar: Terminating the Provider Relationship with a Non-Compliant Patient

It's a dilemma. When a provider-patient relationship breaks down due to poor patient behaviors such as frequently missed or cancelled appointments, refusal to obtain needed screenings, persistently rude or threatening behaviors, then the relationship may need to be terminated.

Connie Christian, MBA, CPHRM,
KaMMCO's Facility Risk Management and Patient Safety Advisor

On Thursday, March 15, Connie Christian, MBA, CPHRM, KaMMCO's Facility Risk Management and Patient Safety Advisor, will present: **Terminating the Provider Relationship with a Non-Compliant Patient** from 12:00 p.m.-1:00 p.m.

This webinar will discuss considerations needed prior to terminating the provider-patient relationship including the review of documentation, communication, timing, behavior contracts, and other special circumstances. The presentation will also cover the termination notification, and plans for developing a formal patient termination process.

As part of KaMMCO's Spring Education Series, this webinar is ideal for clinic and hospital administrators, risk managers, office and support staff, and other interested healthcare professionals.

To register for the March 15 webinar, click here. Registration for the two additional spring webinars (listed below) will be available soon at www.KaMMCO.com/Events.

KaMMCO Reschedules February 22 Webinar for March 29

Due to inclement weather, the February 22 webinar, 'Setting Up a Shared Infection Prevention Program' was cancelled and has been rescheduled for Thursday, March 29 from 12:00 p.m. to 1:00 p.m.

Are you optimizing opportunities to work with community partners? Have you considered expanding capacity in a non-billable service line? Thanks to recent changes in nursing home infection prevention regulations, partnering with a local nursing facility presents an opportunity to expand capacity in both your facility and theirs.

Presenters Nadyne Hagmeier, RN, QI project manager, and Johnathan Reeves, RN, QI project manager, from the Kansas Foundation for Medical Care, Inc., will present a conceptual model of cooperation that leverages hospital knowledge to meet the needs of both nursing homes and your organization.

At the conclusion of the program, attendees will be able to:

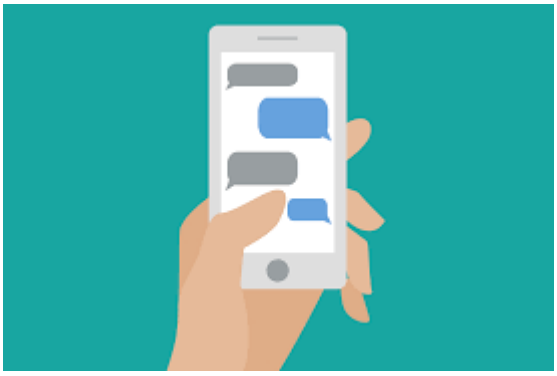
- Understand the difference between hospital and long term care infection prevention requirements.
- Discuss and consider the framework of a shared infection prevention model.

If you were registered for the February 22 event, you will automatically be re-registered for March 29, and you will receive the sign-in information by email from KaMMCO's education coordinator.

To register as a new attendee for the March 29 webinar event, click here.

CMS says "Do not text physician orders"

Connie Christian, MBA, CPHRM
KaMMCO Facility Risk Management & Patient Safety Advisor



In an effort to clarify the Centers for Medicare & Medicaid Services' (CMS) position as it relates to texting, providers need to understand CMS does not permit the texting of orders by physicians or other healthcare providers.

The practice of texting orders from a provider to a member of the care team is not in compliance with the Conditions of Participation (CoPs) or Conditions for Coverage (CfCs). In its Memorandum to State Survey Agency Directors, S&C 18-10-ALL, dated December 28, 2017, CMS warned all texting of patient orders is prohibited, regardless of whether a secure platform is used to relay the orders.

CMS states Computerized Provider Order Entry (CPOE) is the preferred method of order entry by a provider. CMS has held to the long-standing practice that a physician or Licensed Independent Practitioner (LIP) should enter orders into the medical record via a hand-written order or via CPOE. An order entered via CPOE, with an immediate download into the provider's electronic health records (EHR), is permitted as the order would be dated, timed, authenticated, and promptly placed in the medical record.

Other patient information may be communicated via text messaging if the information is sent on a secure platform. CMS recognizes the use of texting as a means of communication with members of the healthcare team has become an essential and valuable means of communication among the team members. In order to be compliant with the CoPs or CfCs, all providers must utilize and maintain platforms that are secure, encrypted, and minimize the risks to patient privacy and confidentiality as per HIPAA regulations and the CoPs or CfCs. It is expected that providers will implement procedures that routinely assess the security and integrity of the texting platforms, and to avoid negative outcomes that could compromise the care of patients.

Through a specialized app, Kansas Medical Society (KMS) members can securely exchange patient information. DocbookMD is a HIPAA-compliant messaging solution designed to facilitate the exchange of protected health information via a smart phone, tablet or laptop. Learn more about DocbookMD at www.docbookmd.com. If you have questions, contact KMS at 800.332.0156

The full text of CMS' Memorandum can be found at www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-18-10.pdf.

A Checklist Worth Revisiting: HHS's Cyber-Attack Quick Response Checklist

Yolanda Sims, JD, HMA,
KaMMCO Loss Prevention & Risk Management Advisor

Healthcare cyber-attacks are still on the rise. Experts in the field say entities should remain vigilant and have a proactive plan in place.

In June 2017, the Department of Health and Human Services (HHS), Office of Civil Rights (OCR) released a quick response checklist and infographic to highlight a series of necessary actions in the event of a cyber-related security incident. Only a few months into 2018, and it bears revisiting the checklist. Studies show that ransomware attacks are more prevalent now than ever before, and employees continue to be the weakest link in cyber security.

The steps outlined here, in brevity, should be done in the event of a cyber-attack or similar emergency.

- Respond Quickly: The entity must execute response and mitigation procedures and all contingency plans. The entity should immediately fix any technical or other problems to stop the incident, and take steps to mitigate any impermissible disclosure of protected health information. In addition, outside vendors (business associates) can be brought in to help.
- Report the Crime: The entity must report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule.

- Report the Threat: The entity should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information.

- Report the Breach: The entity must meet its reporting obligations and individual and/or media notification obligations in a timely manner and required by OCR. According to the guidance, "OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach."

To review the entire checklist and infographic, please visit www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf and www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif.

As a KaMMCO member, you have Cyber Security Insurance (CSI) which covers: network security and privacy violations; both online and offline media; asset protection for recovery or replacement of data; reasonable costs for legal, public relations, credit monitoring, etc.; expenses resulting from extortion; and income loss or interruption due to a terrorism attack.

Visit www.kammco.com/Insurance/Cyber-Security-Insurance to access updated and enhanced online resources to: train employees; conduct a risk assessment; build an incident response plan; implement policies; and manage vendor/business associate risks.

For more information or to speak with someone regarding Cyber Security Insurance, contact KaMMCO Underwriting, 800-232-2259.

Tips from the Trenches: Claims Update

By Cristy Anderson, JD
KaMMCO Vice President, Claims

Specialty: Dental

Procedure: This patient with a history of nighttime teeth grinding, missing five teeth, wearing a partial for the past seven years and prior bridge work, presented to our insured dentist for a consultation regarding the possibility of mini dental implants. The dentist recommended mini implants be installed and suggested the patient did not need to have conventional dental implants. Seven mini implants were installed in March. The patient followed up quite frequently following the procedure for education and check-ups. Over the next two years, the patient developed complications which included multiple failures and repairs of the implants. The patient was reportedly told the complications were due to improper dental hygiene and teeth grinding. The patient sought a second opinion from another dentist who opined the patient was not a candidate for mini implants. The second dentist replaced the mini implants with traditional dental implants. Our insured attempted to settle this claim on his own prior to litigation and wrote several "to whom it may concern" letters explaining the care he provided and stating opinions as to why the procedure failed.

Allegations: The Plaintiff alleged our insured dentist was negligent in using mini dental implants for an unintended purpose and since the patient grinds her teeth, mini dental implants should not have been offered as a treatment option.

Resolution: With our insured's input, this claim was settled.

Risk Management Tips:

- Carefully consider which treatment option is best under the circumstances despite what the patient requests. Sometimes the patient may want to have quick results but the more involved treatment option may be the most effective.

- Sometimes it may be best to refer a patient for a second opinion when more than one attempt has been made at repair. The patient might take this as a sign of strength in the provider rather than weakness thus, preserving the relationship and limiting liability.

- Working with the patient to resolve an issue prior to litigation can have positive results when handled properly. Furthermore, settlements paid out of the providers own pocket are not reportable to the National Practitioner's Data Bank. However, reporting the claim to KaMMCO and allowing KaMMCO professionals to assist you in the resolution may be the most prudent way to resolve a claim. Out-of-pocket, non-reportable, payments can still be arranged.

- Writing a letter to the patient's attorney stating your opinion of your own care could, and most likely would, be used against you.

MIPS Reporting Deadlines Fast Approaching

Deadlines are fast approaching to submit data for the 2017 Merit-based Incentive Payment System (MIPS) performance period. Don't wait until the last minute to submit your data. The two key dates are: March 16 at 8 pm Eastern time for group reporting via the CMS web interface; and March 31 for all other MIPS reporting, including via qpp.cms.gov.

If you are an eligible clinician, here are the top 10 things you need to know. This list focuses on reporting via the qpp.cms.gov data submission feature, **not** on group reporting on the CMS Web Interface and not on individual reporting on Quality measures via claims submission data.

1. Visit qpp.cms.gov and click on the "Sign-In" tab to use the data submission feature.

2. Check that your data are ready to submit. You can submit data for the Quality, Improvement Activities, and Advancing Care Information performance categories.

3. Have your CMS Enterprise Identity Management (EIDM) credentials ready, or get an EIDM account if you don't have one. An EIDM account gives you a single ID to use across multiple CMS systems.

4. Sign in to the Quality Payment Program data submission feature using your EIDM account.

5. Begin submitting your data early. This will give you time to familiarize yourself with the data submission feature and prepare your data.

6. The data submission feature will recognize you and connect your NPI to associated Taxpayer Identification Numbers (TINs).

7. Group practices:
    a. A practice can report as a group or individually for each eligible clinician in the practice. You can switch from group to individual reporting, or vice versa, at any time.
    b. The data submission feature will save all the data you enter for both individual eligible clinicians and a group. CMS will use the data that results in a higher final score to calculate an individual MIPS-eligible clinician's payment adjustment.
8. You can update your data up to the March 31 deadline. The data submission feature doesn't have a "save" or "submit" button. Instead, it automatically updates as you enter data. You'll see your initial scores by performance category, indicating that CMS has received your data. If your file doesn't upload, you'll get a message noting that issue.

9. You can submit data as often as you like. The data submission feature will help you identify any underperforming measures and any issues with your data. Starting your data entry early gives you time to resolve performance and data issues before the March 31 deadline.

10. For step-by-step instructions on how to submit MIPS data, check out this video and fact sheet.

If you are in an ACO or other APM, work with your ACO or APM to make sure they have any patient information they need to report. Remember, you need to report on Advancing Care Information (ACI) measures on your own.

As you plan ahead for 2018, ACI and Improvement Activities are extractable reports from the KaMMCO analytics dashboards. In addition, the CMS-approved Doctors Quality Reporting Network is a Qualified Clinical Data Registry that marries the collection of patient data and the submission of data to CMS. For more information on the analytic dashboards and the DQRN, visit www.khinonline.org/, or contact Susan Penka, spenka@kammco.com, 800.232-2259.

Questions about your participation status or MIPS data submission? Contact the Quality Payment Program Service Center by: Email: qpp@cms.hhs.gov or Phone: 1-866-288-8292 (TTY: 1-877-715-6222).

Note: If you're not sure if you are required to report for MIPS, enter your National Provider Identifier (NPI) in the MIPS Lookup Tool to find out whether you need to report. Additionally, if you know you are in a MIPS APM or Advanced APM, you can use the APM Lookup Tool.

Community HealthCare System's emphasis on cancer screenings delivering results

At Community HealthCare System (CHCS), in NE, Kansas, overall patient wellness has long been a priority. During the Spring of 2017, their seven clinics (and 20 providers) identified a need to emphasize colorectal and breast cancer screening, and began reviewing patient data to identify those who were non-compliant. Clinical preventive services, such as disease screenings, are key to improving the health of the public and offer an opportunity to save years of life. Despite this, many individuals go without clinical preventive services that could protect them from developing serious diseases.

CHCS decided to take action. Utilizing the PDSA (Plan-Do-Study-Act) process to identify cause and strategies, they began by mailing screening reminder letters, making telephone calls to patients in the over-50 age demographic, and implementing an advanced scheduling process for wellness visits.

"At CHSCS we strive for truly patient-centered care," said Melissa Talley, Director of Information Technology and Specialty Clinic Manager. "The annual wellness visits are a huge part of that. Getting patients in the door as part of early detection efforts is crucial."

To address the issue, when a patient arrived for their wellness visit, they were automatically scheduled for their next annual wellness visit at check-in. Staff also scheduled any applicable testing such as mammography or colonoscopy, for which patients receive reminder calls two weeks prior to appointments.

CHCS studied patient access to mammography and colonoscopy services throughout the system, realizing an opportunity to increase access to both procedures in two of their highest volume clinics by adding mobile mammography services and increasing anesthesia services to stabilize the provision of colonoscopies.

Post-implementation of the process changes, CHCS looked closely at compliance rates over a three month period. The newly-implemented strategies positioned CHCS to realize a 3 percent increase in colonoscopies (going from 68 to 71 percent) and a 13 percent increase in mammogram screenings (going from 69 to 82 percent). These screening rates exceed the targets established by Healthy People 2020, a national initiative that highlights the importance of monitoring the incidence of invasive cancers and late-stage breast cancer.

Per HealthyPeople.gov, these types of preventive services not only reduce cancer mortality, but also can save money by helping people avoid unnecessary tests and procedures down the road. The U.S. Preventive Services Task Force recommends having a mammogram every two years, beginning at age 50 for women, and having colonoscopies beginning at age 50 for both men and women.