Exemption Application Open for Quality Payment Program – Avoids 9% Penalty

For providers who are required to participate in the federal government's Quality Payment Program, the exemption application is open for the 2023 reporting year. The government is allowing COVID-19 to be the basis for the exemption. Why bother? If you are required to participate in the program based on your Medicare volume, you must either report or apply for the exemption to avoid the 9% penalty on all Medicare reimbursement in 2025. To double check on your participation requirement, go to https://qpp.cms.gov/ and enter your National Provider Identifier (NPI).

To determine if your 2023 Medicare payments are being penalized for Performance Year 2021, ask your billing team to print off a Medicare remittance. If you see the remark code, CARC 237, you are currently being penalized for failure to successfully participate in the QPP - or declare an exemption. (Claims adjustment reason code 237 is used to denote “Legislated/Regulatory Penalty.")

To apply for the exemption, go to: https://qpp.cms.gov/mips/exception-applications. The application deadline for 2023 is 8 p.m. EST on January 2, 2024. The application takes minutes and can save you tens of thousands of dollars in penalties. If you change your mind and decide to report on the appropriate measures, your application is voided. There is no downside to applying, so don't delay.

2024 Medicare Proposed Rule Reveals Insight

On July 13th, the Centers for Medicare & Medicaid Services (CMS) issued the calendar year (CY) 2024 Physician Fee Schedule (PFS) proposed rule. The ruling is just a proposal, but history demonstrates that it closely aligns with the final policy for the coming year. Therefore, it's worthwhile to evaluate the announcement.

The overall Medicare reimbursement rate will be lowered by 3.34%, as proposed. The 2024 conversion factor is set to be $32.75, a decrease of $1.14 from the CY 2023 conversion factor of $33.89. Note that the proposed rate is typically "improved" by Congressional intervention, but the decline will likely only be softened, not reversed.

In a somewhat surprising move, the government is expanding payment opportunities to practices for non-traditional services. This includes reimbursement for:

- Caregiver training services to support patients when furnished by a physician, advanced practice provider, or therapist – to assist the patient with carrying out treatment plans.

- Health workers supporting Community Health Integration (CHI) services particularly in underserved communities.
- Principal Illness Navigation (PIN) services for the treatment of serious, high-risk illnesses including cancer.
- Peer support and recovery coaches; additionally; marriage and family therapists; mental health counselors; and addiction counselors (that meet applicable requirements) can enroll in Medicare and be paid for their services; these professionals may also use the revised Behavioral Health Integration (BHI) codes.
- Psychotherapy for crisis services; payment is boosted when performed in a patient's home or other non-facility settings, other than the office.
- Social Determinants of Health (SDOH) risk assessments in conjunction with an office visit or the Medicare Annual Wellness Visit (AWV), with an additional payment; proposed to be on the telemedicine-appropriate covered list.
- Health and well-being coaching services to be added as payable when performed via telemedicine.

Further, the government announced its suspension of the Appropriate Use Criteria (AUC) program, even rescinding the current AUC program regulations.

In 2020, the government had proposed payment for an add-on code – G2211 - to evaluation and management (E/M) visits to recognize the "value and inherent complexity in primary and longitudinal care." At the time, the estimated government payout was deemed too high for the budget to bear, so the proposal was scrapped by Congress. The Biden/Harris administration has resurrected the idea. The code, as proposed, could be added onto E/M encounters for a payment boost to recognize "longitudinally treating a patient's single, serious, or complex chronic condition." It may not be used when an E/M encounter is billed with a -25 modifier (to indicate a distinct, separately identifiable service), however, the proposed language provides for broad use. If finalized, expect to receive more details about how and when to use the new code.

As proposed, the government will hold steady on split/shared E/M visits, allowing the current definition of substantive portion to stand. Under the current definition, the billing provider must complete one of the three key E/M visit components (history, exam, or medical decision-making [MDM]), or more than half of the total time spent by the physician and NPP performing the split or shared visit.

Not surprisingly, CMS announced its intention to implement provisions of the Consolidated Appropriations Act 2023 related to telemedicine. This includes, but is not limited to, coverage and payment of the current Medicare telehealth services list through the end of 2024. Further, the telemedicine payment rate is proposed to continue to be the non-facility (higher) rate for professional services.

CMS is proposing to allow academic health systems an exception to the in-person teaching physician requirements for residency training sites. The government is seeking comments as to their proposal that attending physicians can be present for the key portion of the service through audiovisual real-time communications technology.

For more information, peruse the 2,033-page ruling available here – or perhaps just read the much shorter accompanying fact sheet. Expect the final ruling to be issued the first week of November 2023.

When PHI Walks Out the Door with a Departing Employee

Several recent closed cyber claims involve a similar scenario: An employee[1] leaves the employment of a clinic, often on a voluntary basis. Several days or weeks later, the clinic receives reports from existing patients that the former employee is contacting the clinic's patients and encouraging them to seek care at the former employee's new or prospective location. After an investigation, it is discovered that the former employee continues to have access to some information about the clinic's patients. Given the sustained high rate of turnover in the healthcare industry, these scenarios are likely to continue.

While not all these scenarios result in a reportable breach, most involve the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule. As a result, an investigation and assessment must be conducted to determine whether notification to patients, HHS, and perhaps the media is required under the HIPAA Breach Notification Rule.[2] There are several steps that medical groups can take before, during, and following an employment relationship to reduce the privacy and data security risks associated with a staff member's departure.

At the time a new employment relationship begins, the prospective or new hire should be presented with a confidentiality statement to sign that includes an agreement to return any devices, data, or other information the employee has access to during the term of employment. While the specific terms of such an agreement should be drafted in consultation with the group's legal counsel, generally, the individual should agree to perpetually maintain the confidentiality of any PHI that the individual encounters or has access to during or after the term of employment. Additionally, a prospective or new hire should agree not to use or attempt to access any PHI maintained by the group at any time following separation from employment.

Some privacy and data security practices that medical groups should be routinely performing may help discourage employees from intentionally taking PHI with them following the term of employment and may also reduce the risk of individuals doing so inadvertently. A fundamental component of a comprehensive security risk analysis includes performing a complete inventory of all devices and media where PHI is stored. Relatedly, an updated list of all accounts assigned to current employees who have access to PHI should also be maintained. The inventory and account list should be regularly reviewed to confirm that a device or account assigned to an individual who is no longer employed has been promptly addressed. Groups that allow employees to utilize their personally owned devices ("BYOD") to create, store, and transmit PHI should have a clear BYOD policy in place stating, among other things, how the devices will be controlled by the group and an understanding from the employee that any PHI on the device will be remotely wiped at the time of employment separation.[3] Of course, in order to remotely erase a mobile device, the group must have some control over the device through a mobile device management service. In some contexts, groups may consider deploying a data loss prevention (DLP) solution to help enforce administrative policies addressing improper retention or transfer of sensitive data. As required by the HIPAA Security Rule, covered entities should also regularly review their procedure for information system activity review (e.g., an audit log review) and confirm that the procedure is properly in place. As part of initial and recurring training, as well as in periodic security reminders, a group should be clear about its system activity review efforts. Among other benefits in such transparency, an enterprising, perhaps soon-to-be-former-employee may think twice about accessing and copying patient information if he or she knows that such activity is subject to being monitored.

Medical groups should have comprehensive policies in place about the various steps, including those related to information security, to be taken at the time of employment separation, regardless of the reason for the end of the employment. When an employee has given notice of their intention to resign or if an employee has been terminated, a spot check of their activity over the preceding days or weeks in the electronic medical record may reveal an anomalous pattern of use which may give rise to further investigation. Following the departure of a staff member, healthcare providers within the group should also be alert for unusual reports from patients about contacts from the former employee or unknown telephone numbers. In the event that the group discovers an indication of an improper access or acquisition of PHI, including information which may still be in the

possession of the now-former employee, the group should initiate its incident response policy for investigation into the matter.

Hackers are not the only source of privacy and data breaches. Medical groups must have safeguards in place to reduce the risks of privacy and security incidents caused by current employees, as well as staff members that are leaving the employment of the group, regardless of the reason.

If you experience a cybersecurity or other HIPAA-related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage® account here.

[1] Many state medical boards have rules addressing patient notification of a physician's departure from a group. For example, in Tennessee, the applicable rule provision addressing records of physicians upon departure from a group provides that "the responsibility for notifying patients of a physician who leaves a group practice whether by death, retirement or departure shall be governed by the physician's employment contract." The rule also provides criteria regarding which patients must be notified, and the content of the notification. Physicians should be familiar with the relevant provisions for patient notification in their employment agreements. Likewise, groups should know how to properly execute these provisions in the event of a physician departure, while also remaining mindful of their obligations under the HIPAA Privacy and Security Rules for safeguarding PHI (which includes patient name and contact information).

[2]. These instances may constitute a security incident. For obligations related to responding to such an incident, see the article, "Obligations of Medical Practices in Responding to Data Security Incidents (Not Just Data Breaches)." Even for those situations not constituting a security incident, such as incidents involving paper form PHI, the requirements are similar in the context of the HIPAA Breach Notification Rule's presumption that any an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule is (with few exceptions) presumed to be a breach.

[3]. Employees should also understand that devices they personally own but are managed by the group will be remotely erased in the event the device is lost or stolen.

Risk Matters: Physician-Patient Relationships

With school starting back and fall sports practices commencing, many physicians and providers will be asked to perform a sports physical to provide medical clearance for student athletes to participate in sports activities. Most jurisdictions will find that even a single encounter for the limited purpose of performing a sports physical creates a physician/provider - patient relationship. Often a physician/provider who is asked to perform the physical has no prior history with the patient and limited medical information. Therefore, it is important that the physician/provider obtain a detailed history from the patient (and parent if possible) and perform a thorough exam on the student athlete. Primary areas of concern should be prior injuries, respiratory function, concussion risk, and conditions which might lead to cardiac arrest. Sports physicals should never be considered perfunctory exams. The bottom line is do not merely rubberstamp the clearance certificate, or you may be at risk of a malpractice claim.

---

attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.