Sample Medication Management

By Jeffrey A. Woods, JD

It is common practice for physicians and providers to dispense free sample medications to patients. The benefits of dispensing sample medications are numerous: it allows patients to try new medications on a trial basis; saves patients money on expensive medications; reduces non-adherence to medication regimens; expedites getting prescription medications into the hands of patients; and can strengthen the physician-patient relationship. But, as with most everything you do, there are risks.

As with any new medication, adverse reactions and/or side-effects are a possibility, but with sample medications there is no pharmacist safety net. Similarly, there is often no package insert or handout that provides patient education, instructions, or safety warnings. Therefore, it is solely incumbent upon the physician/provider to educate, instruct, and warn the patient about these things. The duty of care owed to patients is no less when dispensing sample medications than it is when writing prescriptions.

Moreover, sample medications require the same level of security and accountability as their prescription counterparts. Lack of proper storage, security safeguards, inventory

documentation, and sample medication policies can lead to additional risks. Allowing access to the sample medication storage closet by staff can result in misuse and diversion of drugs to family and friends without up-to-date documentation and routine audits.

Finally, a lack of documentation relative to dispensed samples, including manufacturer, lot number, expiration date, and quantity can be problematic in the event of a drug recall.

To minimize these risks, do the following:

1. Familiarize yourself with all state and Federal laws and regulations relating to sample medications.
2. Have a written policy for handling and dispensing sample medications including storing, securing, logging, tracking, documenting, and dispensing.
3. Store sample medications per the manufacturers' recommendations and monitor expiration dates.
4. Create a log documenting the name, manufacturer, quantity received, receipt date, lot number, expiration date, quantity dispensed, date dispensed, and name of the recipient.
5. Dispense sample medications only through licensed physicians/providers who have prescriptive authority.
6. Document in the patient's medical record the intended purpose for the medication.
7. Provide patients with appropriate education, instructions, and safety warnings (including informed consent where applicable) specific to each medication dispensed and thoroughly document these discussions.
8. Document with specificity in the patient's medical record each sample medication dispensed including the name, quantity, manufacturer, lot number, and any follow-up instructions.
9. Have a plan for notifying patients of manufacturer recalls.
10. Dispense sample medications to family, friends, and colleagues only when a medical record has been established for the patient and subject to any applicable ethical rules and regulations.
11. Label samples in accordance with state and federal guidelines.
12. Pharmaceutical representatives should not be allowed access to the storage area without staff being present.

If you have any questions, please contact SVMIC at 800.342.2239 or by email at ContactSVMIC@svmic.com.

Cyber Education is More Than a Meeting

By Rana McSpadden, FACMPE

A practice does not need to implement the most expensive technology or hire full-time IT staff in order to comply with the HIPAA Security Rule. So long as policies and procedures, technology, and physical safeguards which are appropriate for the size of the practice are put in place, compliance is achievable. However, if staff members are not trained in their role in the prevention of cybersecurity incidents, all other prevention measures may be for naught. Staff are on the front lines of cybersecurity and, without the proper knowledge and skills to recognize risks, may leave themselves and the practice vulnerable. Firewalls cannot prevent hackers from accessing systems if staff members inadvertently give them their login credentials or download malware through infected links sent through a phishing email. Device encryption is futile if staff members do not log out of the system before walking away from their workstation or laptops, allowing someone to walk up and access anything in the system.

In addition to HIPAA privacy education, security awareness and training should also be

provided to all members of a practice's workforce.

Who should receive education?

Every member of the practice workforce should receive education. This includes staff, management, and providers. Anyone who has access to the practice's systems, including any temporary staff or students, should receive education on their role in preventing cybersecurity incidents.

How often should education be provided?

As with general HIPAA education, all new workforce members should receive education as soon after hire as possible. Additionally, re-education for all members should be performed on a periodic basis as well as when there are changes in policies and procedures, whenever new software or hardware is implemented, or if changes are made in the Security Rule. It is best practice to do security awareness training at least annually. Educational calendars are an easy way to stay abreast of training and provide reminders. To supplement and reinforce education efforts, the security reminders and updates should be provided periodically throughout the year and whenever there is a security incident. These reminders should be brief and provide timely information regarding security risks to the practice.

What should be included in education sessions?

Some of the most important topics that should be covered in cybersecurity education relate to ways in which workforce members can guard against, detect, and report malicious software. Topics include (but are not limited to) how to spot a phishing email, the risks of clicking suspicious links, the dangers of downloading infected files, and to whom to report suspicious activity. This point of contact may be the HIPAA Security Officer, a manager, or IT personnel. Additional education may focus on processes or software used to report suspicious emails or activity. Other topics may include information about various threats to practice systems and why they are a threat, such as ransomware. Additionally, workforce members should be educated on log-in monitoring to thwart inappropriate log-in attempts, what happens when there are too many log-in attempts, and how to manage passwords. Password management education should discuss the use of complex passwords, how to change passwords and how often passwords should be changed, as well as the dangers of keeping written passwords in the open or sharing them with others. A practice's security policies and procedures may provide a good place to start for an outline of topics to cover, as well as providing some of the content to be presented.

How should education be provided?

There are several ways to provide cybersecurity education and reminders to all members of the workforce. Full education can be provided through formal educational presentations or webinars. Routine security reminders can be provided using memos, postings in employee areas, email blasts, newsletters, or during monthly staff meetings. Whatever

format is used, it should be what benefits the practice and workforce most. As with other areas of a practice's HIPAA compliance program, retain documentation of education efforts, including the content presented, date presented, presenter information, and to whom it was presented. To assist with practice education needs, SVMIC provides multiple resources on our website as well as through Cybernet. To access these resources, click here. If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity 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.

Standing Firm

By Randa Gibson, JD

Barbara Jones[1], a 60-year-old female patient, presented to her local ER in Arkansas with acute onset abdominal pain and some distention. The history taken by the ER physician revealed a prior gastric bypass surgery and hernia repair surgery two years previously. A CT scan showed probable partial small bowel obstruction changes.

Dr. Abbott was the hospitalist that evening. He accepted the patient for admission around midnight and performed an examination. He was aware of the history of gastric bypass, as well as the CT findings and reports of acute onset abdominal pain, nausea, and bloating. He made a plan for the patient, which included bowel rest, fluids, and an NG tube. He did not feel that there was a need for a general surgery consultation at admission but documented that if there was no improvement, the patient would need one.

The following day, a different hospitalist, Dr. Brand, assumed care of the patient. She did not change the plan for the patient and, like Dr. Abbott, did not order a surgical consult. A third hospitalist, Dr. Calhoun, took over the patient's care on day two and managed her through discharge. Like Dr. Brand and Dr. Abbott, Dr. Calhoun did not order a surgical

consult. At trial, both would explain that this was because the patient had continually improved – her abdominal pain resolved, she had bowel movements, and she tolerated diet advancement.

Not long after being discharged, the patient saw her PCP for a follow up, reporting abdominal pain and lack of bowel movements. The PCP requested the patient notify her if her symptoms persisted and ordered abdominal x-rays, which showed evidence of a distal small bowel obstruction.

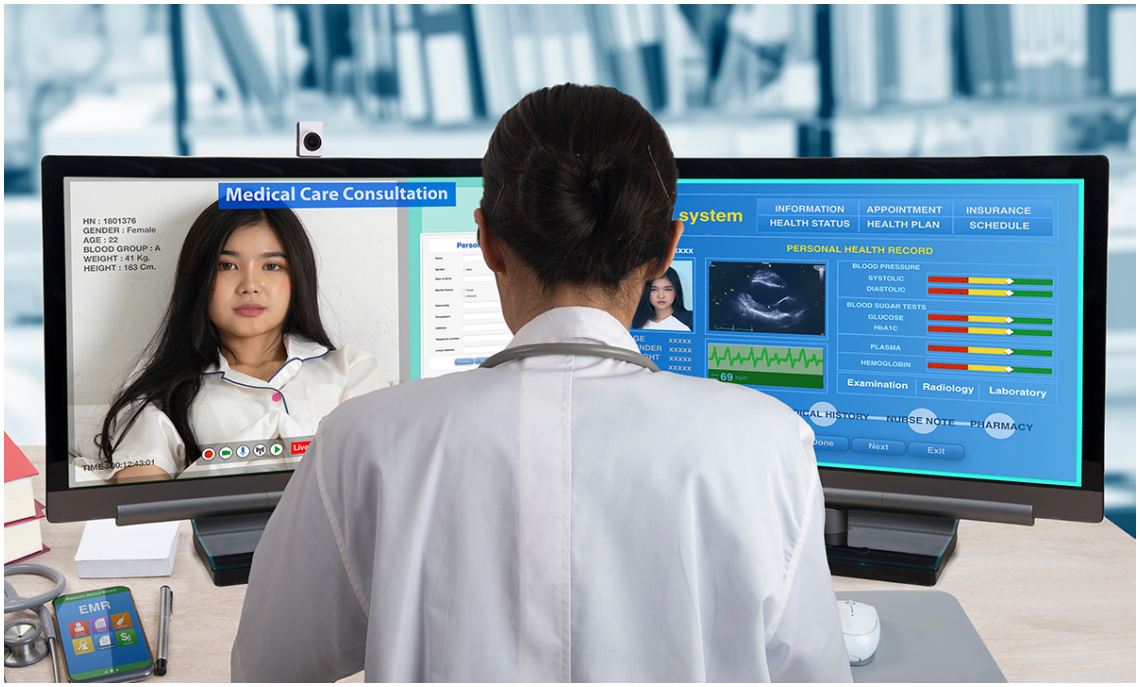
The following day, the patient saw a physician affiliated with her gastric surgeon for a routinely scheduled follow up. She reported the history above to the physician, but also that she was feeling better. He, like the PCP, allowed the patient to go home, and instructed her to let him know if her symptoms worsened or reoccurred. After sending the patient home, however, the provider consulted with a gastric surgeon, who advised him to have the patient return to the hospital for an exploratory laparotomy for a possible internal hernia. When the surgery was performed on the patient two days later, a perforation occurred. The patient developed complications postoperatively, including sepsis. Following a lengthy hospitalization, second surgery, and rehabilitation, the patient recovered to baseline, but not before incurring significant medical expenses.

The patient elected to file suit against the three hospitalists, her PCP, and their employers. By the time of trial, the only defendants were the three hospitalists, the patient dismissing the PCP earlier on in the case. The patient's theory? That each hospitalist should have ordered a surgical consult during the admission. The Plaintiff had an expert to testify that a routine surgical consult should have been ordered by Dr. Abbott, Dr. Brand, and Dr. Calhoun. The Plaintiff also called one of the patient's treating gastric surgeons, Dr. Zeigler, who testified at trial that he would have returned the patient to the OR during the original admission had he been consulted. He testified that this earlier intervention would have led to less compromise of the bowel and the perforation would not have occurred.

It can be especially intimidating to defend your care through trial when it is criticized not only by outside experts, but also by a treating physician. But here, despite the uncertainties of trial, all three defendants held their ground and defended their care, supported by strong experts who agreed that the standard of care did not require surgical consultation in this patient, that a trial of medical management was appropriate, and that the perforation was not related to any treatment, or lack thereof, by the defendants. The defendants' confidence in the care they rendered was not misplaced, as the jury found that each met the standard of care. The plaintiff recovered nothing, and the case was closed.

1 Names have been changed throughout this claim.

New Federal Law Extends Telemedicine Reimbursement



By Elizabeth Woodcock, MBA, FACMPE, CPC

Performing telemedicine in your practice is an operational challenge, but those challenges pale in comparison with the unknowns about its reimbursement in the long run. Prior to the COVID-19 pandemic, telemedicine was not on the radar for most medical practices, but today it's standard industry practice to offer services via telemedicine. However, questions remain about its future as reimbursement has been largely tied to the government's public health emergency (PHE) during the pandemic. While changing the law to establish permanency for telemedicine is a challenge amidst today's political agenda, the government has managed to bolster key elements of reimbursement – at least for the time being.

On March 15, President Biden signed the Consolidated Appropriations Act (CAA) 2022 into law, allowing for these flexibilities related to Medicare reimbursement for 151 days after the PHE concludes:

- Services may be provided to Medicare patients at any location, including their home.
- Occupational and physical therapists will continue to be able to furnish and be reimbursed for telemedicine services; speech pathologists and audiologists are also included as eligible clinicians.
- Audio-only technology will continue to be permitted for office visits, and any other services not requiring the use of interactive, real-time equipment.
- Federally qualified health centers (FQHCs) and rural health clinics (RHCs) can continue to provide telemedicine services.

As of April 16, 2022, the current PHE has been extended for another 90 days. The law called for MedPAC, the independent advisors to Congress, to assess the issue of telemedicine reimbursement. In the spring of 2021, MedPAC issued a report that reimbursement should be rolled back to a pre-pandemic state, but consumer expectations have changed substantially since then.

If you have questions about telemedicine and reimbursements or your malpractice insurance coverage related to telemedicine, please don't hesitate to contact SVMIC at 800.342.2239 or ContactSVMIC@svmic.com. Members can also find further details on telemedicine and reimbursements on our Vantage portal.
