A Patient’s Wandering Eye and the Internet Can Lead to Pump Tampering

Matthew Grissinger, RPh, FASCP

Mr. Grissinger is Director of Error Reporting Programs at the Institute for Safe Medication Practices in Horsham, PA (www.ismp.org).

PROBLEM: A hospitalized patient with chronic pain was able to increase the rate of his hydromorphone infusion and to self-administer bolus doses according to the code used by clinicians in the facility. The patient had been receiving hydromorphone via a CADD-Prizm VIP pump (Smiths Medical) at home before he was admitted to the hospital late one evening. The admitting physician prescribed the same dose of hydromorphone that the patient had been receiving at home and allowed the patient to use his own pump from home while he was in the hospital. The hospital-based pain service team had been following the patient’s care at home but was not notified of his admission until the following morning. That morning, a resident questioned why the patient’s hydromorphone infusion was running at a rate that differed from the rate prescribed.

A member of the pain service informed the resident that the dose had not been changed by anyone on the team and that the patient could not be seen until later in the day because of a busy clinic schedule. The resident did not investigate the change in the infusion rate any further. Eighteen hours elapsed before the pain service physician was able to visit the patient. Nursing documentation was vague on how much medication was being infused compared with how much should have been infused. However, when the physician looked at the history log of the patient’s pump, he quickly discovered that the patient had somehow manipulated the infusion rate and had given himself frequent boluses that had not been prescribed. The staff replaced the patient’s home CADD pump with a hospital CADD pump of a different model and secured the pump with a tackle box and padlock to ensure no further tampering.

It became clear that the patient knew how to manipulate the pump and had obtained and used the lock level (security) code to alter the pump settings and the clinician code to administer bolus doses. But how did he gain this knowledge?

In response to the FDA’s request that information about approved drugs and devices be made more accessible, the user manual for the pump was posted on the manufacturer’s Web site. The site therefore enabled patients to see how to program the pump. However, the codes themselves are not included in Internet sources; they are available only in the hard copy of the user manual that hospitals receive. As a result, the patient might have obtained the lock level and clinician codes from the pump he used at home by observing practitioners while they programmed the pump. A better possibility is that the codes, which are the same for this pump throughout the U.S. (when shipped by the manufacturer), were communicated via the Internet or via e-mail by others.

SAFE PRACTICE RECOMMENDATION: Although there is probably no foolproof way to prevent patients from tampering with pumps that deliver opioids, health care professionals can reduce the risk of tampering or can quickly detect it by following these steps:

1. Shielding and scrolling. When programming a pump, the staff should always block the view of patients and visitors. They should use the scroll-up or scroll-down keys, if available, to prevent patients from counting how many times the keys are pressed.

2. Checks and balances. Home-care and hospital nurses should use carefully designed flow sheets during opioid infusions to track cumulative doses over time (at four-hour increments for in-patients). They should refer to the pump’s history log to compare the prescribed dose.

3. When to probe further. The possibility of patient tampering (or an error) should be considered if the dose or volume administered does not match the prescribed dose or if the patient’s sedation level, respiratory status, or behavior differs from what is expected.

4. Staff education. When showing staff members and other caregivers how to use infusion pumps, the instructor should emphasize ways to minimize the chance that patients or visitors will be able to learn the programming codes.

5. Checking security features. All pumps used for opioid infusions, as well as new pumps being considered for purchase, should be checked to ensure that the locking mechanism for the compartment that holds the medication is functioning and reliable. Patients and visitors have opened the locked compartment by using pens, paper clips, or other objects to push the syringe plunger, syringes with long needles to aspirate the medication, or moderate pressure.

6. Hospital pumps only. To enhance security, only hospital-approved pumps should be used to administer opioids to hospitalized patients. Patients should not be allowed to use their pumps from home.

7. Monitoring opioid use. Pharmacies that supply opioids to home-care patients and hospital pharmacists who dispense these medications should monitor the amount of drug dispensed to ensure that it matches the prescribed doses. Any discrepancies should be investigated immediately.

8. Screening patients. Patients with chronic pain should be carefully screened to verify that they are appropriate candidates for opioid infusions, including patient-controlled analgesia. Patients should be informed that their opioid use will be monitored.

9. Changing codes. Some pumps offer biomedical staff members the ability to change the lock level and clinician codes. Changing the codes temporarily should be considered for patients who appear to be able to tamper with the pumps.

continued on page 328
should be done as long as the new codes can be securely communicated to all practitioners who need the information.

10. **Utilizing a pain service.** If the facility offers a pain service, the team should be notified immediately when a patient with chronic pain is admitted, especially if the patient has been receiving opioids at home.

---

*The reports described in this column were received through the ISMP Medication Errors Reporting Program (MERP). Errors, close calls, or hazardous conditions may be reported on the ISMP Web site (www.ismp.org) or communicated directly to ISMP by calling 1-800-FAILSAFE or via e-mail at ismpinfo@ismp.org.*