Patient abuse of pain management pumps

The Safety and Quality Committee (SQC) of the Australian and New Zealand College of Anaesthetists (ANZCA) has received reports from Australia about patients gaining access to and altering the dosing parameters on pain management medication pumps.

Patients have administered to themselves unprescribed/unprogrammed additional amounts of S8 drugs.

It appears the patients have "learned" the programming codes for the pumps, either by finding them on a publicly available webpage or by simply watching clinicians key in the pump's code.

Clinical personnel have subsequently discovered, upon review of the pump's digital memory, that the patients had delivered drug doses to themselves.

While the patients involved did not come to harm, these incidents have, nevertheless, exposed a significant issue.

In Western Australia, WA Health has directly notified health care services statewide via a Medical Device Safety Notice (attached as appendix).

The SQC recommends the following measures:

- **Health care facilities should re-programme their pain medication pumps so the codes are different to the publicly available default code.**
- **Clinicians should ensure patients cannot learn how to programme pain pump codes via the clinician's actions. For example, by the clinician verbalising the code within earshot, or by indiscreetly programming the pump in full view, of the patient.**

Medical Device Safety Notice

Patient Controlled Analgesia (PCA) Infusion Devices- Risk of Unauthorised Access to settings

This information has been distributed to provide advice to WA health professionals of a potential safety risk. This notification has been created and adapted using the Unauthorised access to Patient Controlled Analgesia Infusion Pumps Safety Notice from New South Wales Clinical Excellence Commission

Issue Date:	**30 May 2025**
Key Message	**WA Health sites need to be aware of an emerging risk where patients have been able to gain access to Patient Controlled Analgesia (PCA) security codes to alter infusion settings**
Immediate Actions	1. Distribute this safety notice to all relevant clinical areas where PCA Infusion devices are used and ensure all staff are made aware. 2. Review and reinforce security protocols for Patient Controlled Analgesia infusion devices 3. Acknowledge and action the required actions 4. Given the content ensure this notice is kept away from areas where it may be publicly observed.

Situation:

- WA Health has been made aware of incidents in another jurisdiction where patients were able to access security codes to unlock PCA infusion devices and alter the infusion settings.
- Whilst there have been no reported incidents in WA Health, proactive measures are required to maintain patient safety.

Background:

- PCA Infusion devices are designed to enable patients to self-administer controlled doses of prescribed analgesia at preset intervals.
- These devices typically include safety features such as security codes to prevent unauthorised changes to dosage parameters. These devices are generally purchased with a default security code/s which are published in the operator's manual and may be accessible in the public domain. Multiple codes may exist for different levels of access and should be customised to prevent unauthorised access through use of default codes.
- As indicated by other jurisdictions, codes may be accessible or predictable, potentially allowing patients to bypass safety controls so staff vigilance is required.

Assessment:

- Unauthorised access to PCA infusion devices poses a significant risk to patient safety. If patients are able to alter infusion settings, it could lead to:
  - Overdosing or underdosing of medication, compromising pain management.
  - Increased risk of adverse drug events.
  - Overriding of pump safety features.

Required Actions:

1. Immediate review of current practice:
   - Audit all PCA infusion pumps to ensure appropriate security settings are in place and codes are not set to default.
   - Consider the use of additional security features if available and not already in place.
2. Device Configuration Check:
   - Verify that all PCA devices have been customised according to manufacturer guidelines.
   - Ensure that access codes are changed immediately from factory defaults and at regular intervals.
3. Staff Education and Vigilance:
   - Confirm that all staff are aware of the importance of maintaining code confidentiality.
   - Reinforce training on PCA device security protocols.
   - Encourage staff to report any unusual patient behaviour or suspected tampering.
4. Ongoing monitoring and Reporting of adverse events:
   - Report any security breach incidents into the local Clinical incident management system (CIMS)

The information in this alert is provided in good faith for the purpose of identifying possible safety issues and risks to facilitate improvements in safety and quality of health care. While every reasonable effort has been made to ensure the accuracy of the alert, no guarantee can be given that its contents are (1) free from error or omissions, or (2) current at the time you access it.
The State of Western Australia, the Minister for Health and the Department of Health and their officers, employees and agents expressly disclaim liability for any act of omission occurring in reliance on the information in the notification and for any consequences of such act or omission.

Contact: Medicines and Technology Unit
Patient Safety and Clinical Quality Directorate
Clinical Excellence Division
Department of Health, Western Australia
E: DoH.MedicinesandTechnology@health.wa.gov.au
W: www.health.wa.gov.au | www.healthywa.wa.gov.au