ISMP Canada Safety Bulletin

Volume 25 • Issue 8 • July 31, 2025

Emergency Preparedness Mitigates Patient Harm during Failed Deployment of Upgraded Automated Dispensing Cabinets

During an upgrade to new automated dispensing cabinets (ADCs, also known as automated dispensing units [ADUs]), a hospital network experienced a serious incident that led to corruption of the ADC medication database and impacted system-wide functionality of the ADCs. This bulletin shares recommended safety measures for facilities undergoing a similar upgrade to ADCs or other technology to prevent patient harm.

> "Technically, the biggest 'safety system' in healthcare is the minds and hearts of the workers who keep intercepting the flaws in the system and prevent patients from being hurt. They are the safety net, not the cause of injury."
>
> **Donald M. Berwick MD MPP FRCP KBE**

BACKGROUND

ADCs are computerized medication storage devices that are commonly used to securely store and dispense medications near the point of care.[1] The use of an ADC offers multiple benefits, including real-time tracking of drug distribution and inventory management, reduction in medication errors, reduction in drug diversion, and efficiencies in medication management.[1] Regular upgrades of ADC software and hardware are required for optimal performance. Certain steps must be followed during the upgrades to ensure proper configuration of the units. Planning ahead can reduce the likelihood and duration of downtime periods related to upgrades.[2,3]

INCIDENT DESCRIPTION

To support the deployment process for an upgrade to new ADCs, the vendor protocol required importing the entire medication database in a single step. Instead, an inadvertent deviation from the protocol occurred, whereby partial importation of the database was completed, followed by a second step to import the remaining medication information. During this second step, the data became misaligned. The misaligned data was then uploaded to the new ADCs and affected the entire ADC network; erroneous medication information was displayed to ADC users (Figure 1).

FIGURE 1. Simplified example of a frameshift error of data importation to an automated dispensing cabinet (ADC).

The pharmacy team was alerted to ADC issues within minutes of the vendor database upload, when nursing staff reported that misoprostol tablets were displayed as 30 mL unit dose cups. A second report described the ADC directing the nurse to a drawer containing morphine 2 mg ampoules, whereas morphine 10 mg tablets had been selected. Following these 2 reports and subsequent investigations, the vendor was engaged; they confirmed that the upload process containing the error could not be immediately aborted. The ADC inventory processes were halted, and real-time support was provided to nursing to obtain the correct medications. An emergency operations centre was initiated, and Code Grey (critical infrastructure loss/failure) was declared across the network of hospitals. It took approximately 6 hours to resolve the Code Grey.

DISCUSSION

This incident affected more than 300 medication products. During the downtime, more than 150 medication transactions were affected. Pharmacy and nursing staff worked collaboratively to ensure that patients received the correct medications at their prescribed doses. No patient harm was reported as a result of the incident.

Two key factors contributed to the incident:
• Deviation from the existing vendor protocol for importation of the medication database, which affected multiple data fields including the drug name, strength, format, quantity, and physical ADC assignment locations
• Launch of corrupted medication data into the live hospital-wide server communicating with ADCs

The organization benefited from the following mitigating strategies that were already in place:
✓ An established pharmacy emergency preparedness plan
  ◦ Pharmacy staff were deployed to care areas to provide in-person support.
    ▪ Pharmacy staff were physically deployed to key clinical areas (e.g., operating rooms and intensive care units) to support urgent clinical cases requiring medications.
    ▪ Pharmacy staff actively monitored nursing ADC transactions and initiated individual calls to confirm accuracy of the medications being dispensed.
    ▪ Pharmacy staff dispensed required medications from the central pharmacy department that were erroneously being dispensed by ADCs.
✓ On-site hospital staff with advanced technical expertise in automation systems
✓ Rapid activation of the emergency preparedness plan and emergency operations centre
✓ Ongoing communication to all affected groups
  ◦ Resolution of the critical issue was communicated hospital wide approximately 6 hours after the first report was received.

RECOMMENDATIONS

The recommendations below include strategies shared by the reporting hospital to prevent or mitigate harm from this type of incident. Many of these strategies were in place by the hospital team and contributed to the successful mitigation of patient harm in this event.
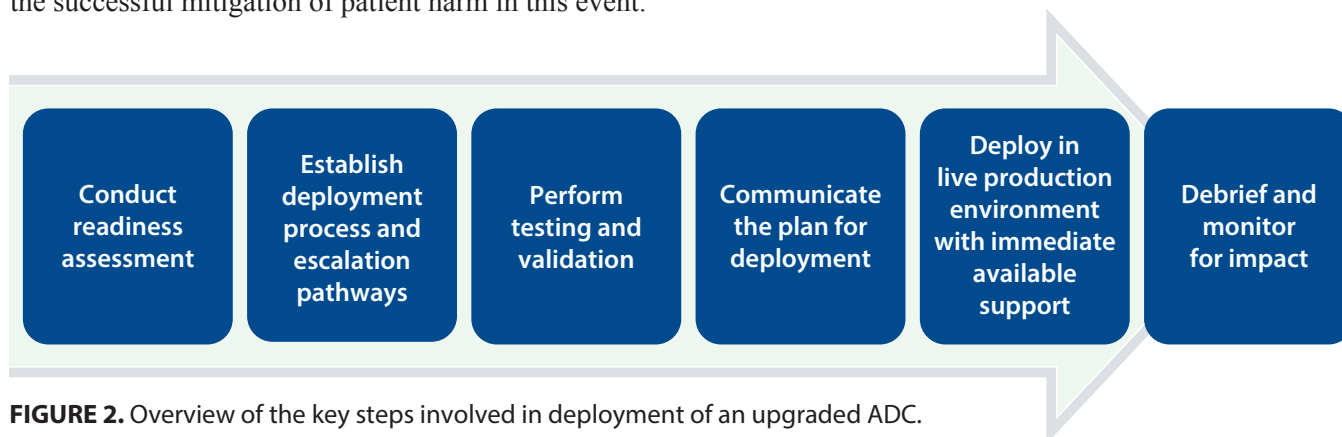
Conduct readiness assessment	Establish deployment process and escalation pathways	Perform testing and validation	Communicate the plan for deployment	Deploy in live production environment with immediate available support	Debrief and monitor for impact

FIGURE 2. Overview of the key steps involved in deployment of an upgraded ADC.

Vendor Teams

- Establish a standard process for deploying technology in heterogeneous hospital environments.
- Build internal checks for illogical data after a database manipulation, such as a tablet being dosed as a volume (e.g., mL). If such discrepancies are detected, the system would ideally pause the upload and alert the vendor and hospital pharmacy informatics teams.
- Ensure that vendor deployment teams have the necessary knowledge and expertise, including the following:
  ◦ Familiarity with the HL7 standard to support integration of data with hospital information systems
  ◦ Ability to provide timely identification, monitoring, and resolution of implementation errors
  ◦ Escalation protocol that can be executed immediately to obtain support
- Conduct a formal, mandatory readiness assessment (hardware, software, workflow impact) for all ADC deployments.
- Host post-deployment debriefs with clients to capture learning from incidents and to inform continuous quality improvement.

  ◦ Share the learning with all clients/stakeholders through incorporation into standard operating procedures to prevent future incidents.

Hospital Teams

- Ensure that the hospital informatics team includes dedicated members from pharmacy, nursing, and risk management, as well as expertise in data field mapping.
- Establish planned and unplanned downtime procedures for key technologies:
  ◦ Create a communication plan to ensure that all affected parties will be updated.[2]
  ◦ Ensure that documented downtime procedures are readily accessible and sufficiently detailed (e.g., step-by-step guide). Ideally, staff are trained and ready to carry out manual processes.[2]
- Ensure that all affected staff are alerted to planned upgrades so that downtime and recovery procedures can be reviewed and additional back-up plans developed, where necessary.
- Ensure a standardized readiness checklist is approved by the vendor, hospital leadership, and the hospital informatics team.

Vendor and Hospital Teams

- Evaluate the potential impact and develop a mitigation plan in the event of a protocol deviation.
- Implement an import process for medication databases that includes the following elements:
  ◦ Testing and validation within a test environment (e.g., using a virtual ADC)
  ◦ Checks to ensure accurate importation
  ◦ Deployment into the production environment only after approval from the hospital informatics team, vendor, and other resources defined by the hospital team
- Establish clear escalation criteria and pathways to ensure timely response to issues raised.
- Report incidents related to technology deployment both internally and externally, to support continuous quality improvement.

CONCLUSION

Changes in technology related to system upgrades can introduce unexpected system failures and downtime. Detailed advance planning and testing can reduce the likelihood of such situations and support rapid detection of system problems to mitigate patient harm. The knowledge and actions of the reporting hospital's dedicated leaders and front-line staff, including activation of the emergency preparedness plan and emergency operations centre, mitigated what could have been harmful medication errors affecting hundreds of patients.

REFERENCES

1. Guidelines for the safe use of automated dispensing cabinets. Plymouth Meeting (PA): Institute for Safe Medication Practices; 2019 [cited 2025 Jun 18]. Available from: https://www.ismp.org/system/files/resources/2019-11/ISMP170-ADC%20Guideline-020719_final.pdf
2. Larsen E, Hoffman D, Rivera C, Kleiner BM, Wernz C, Ratwani RM. Continuing patient care during electronic health record downtime. Appl Clin Inform. 2019;10(3):495-504.
3. Jo I, Kim W, Lim Y, Kang E, Kim J, Chung H, et al. Strategy for scheduled downtime of hospital information system utilizing third-party applications. BMC Med Inform Decis Mak. 2024;24:300.

Report Medication Incidents

(Including near misses)

Online: www.ismpcanada.ca/report/
Phone: 1-866-544-7672

ISMP Canada strives to ensure confidentiality and security of information received, and respects the wishes of the reporter as to the level of detail to be included in publications.

Stay Informed

To receive ISMP Canada Safety Bulletins and Newsletters visit:

www.ismpcanada.ca/safety-bulletins/#footer

This bulletin shares information about safe medication practices, is noncommercial, and is therefore exempt from Canadian anti-spam legislation.

Contact Us

Email: cmirps@ismpcanada.ca
Phone: 1-866-544-7672