Australian Government
Department of Health
Therapeutic Goods Administration

Medical Devices Safety Update

Volume 4, Number 2, March 2016

In this issue

Endoscope reprocessing 'top hazard'

Inadequate cleaning of endoscopes has been named as the top health technology hazard worldwide, followed by clinical alarm hazards

Inadequate cleaning of endoscopes surpassed clinical alarm hazards as the number one health technology hazard worldwide for 2016, according to the Emergency Care Research Institute (ECRI).1

Clinical alarm hazards had topped the ECRI list in 2012, 2013, 2014 and 2015 and placed highly in prior rankings. ECRI's top 10 hazards list for 2016 is:

1. Inadequate cleaning of flexible endoscopes before disinfection may spread deadly pathogens (MDSU articles discussed this issue and related issues in September 2014 and November 2015).
2. Missed alarms may have fatal consequences (an MDSU article discussed this issue in May 2014).
3. Failure to effectively monitor postoperative patients for opioid-induced respiratory depression may lead to brain injury or death.
4. Inadequate surveillance of monitored patients in a telemetry setting may put patients at risk
5. Insufficient training of clinicians on operating room technologies may put patients at increased risk of harm.
6. Errors arise when health IT configurations and facility workflow do not support each other.
7. Unsafe injection practices expose patients to infectious agents.
8. Gamma camera mechanical failures can lead to serious injury or death.
9. Failure to appropriately operate intensive care ventilators can result in preventable lung injuries.
10. Misuse of USB ports can cause medical devices to malfunction.

Focus on solutions

The TGA advises health professionals to consider ways to mitigate risks within the clinical settings in which they work. Health facilities should:

- set up effective risk management programs that involve clinicians, biomedical engineers, hospital management and administrative staff.
- ensure that responsibilities are clearly assigned to the relevant personnel.
- ensure all staff carefully read and fully understand the Instructions for Use for devices they use and are responsible for.

REFERENCE

1. Top 10 Health technology Hazards for 2016, Health Devices, November 2015. Emergency Care Research Institute (registration required)

Medical Devices Safety Update is the medical devices safety bulletin of the Therapeutic Goods Administration (TGA)

TGA Health Safety Regulation

Device cybersecurity a key issue

In recent years cybersecurity experts and regulators worldwide have been focusing on reducing the vulnerability of medical devices to potential hacking, malware and other such attacks

Cybersecurity experts have identified a wide range of medical devices as potentially vulnerable to unwanted intrusion, including technology as diverse as PET scanners, infusion pumps and life-support equipment.

Devices incorporating wireless communications are particularly vulnerable as potential hackers can operate remotely. Common medical devices that use wireless communications include:

- infusion pumps
- insulin pumps
- implantable drug pumps
- implantable cardiac defibrillators
- pacemakers
- neural stimulators
- insulin pumps
- telemetry heart monitors
- infant/foetal monitors.

Although there have been no reports of hacking attacks on medical devices in Australia, there have been reports of such attacks overseas. Cybersecurity experts in Australia have demonstrated a wide range of potential vulnerabilities in simulated attacks.

Defensive measures advised

TGA advises medical device sponsors and asset owners to perform risk assessments by examining the specific clinical use of potentially affected products in the host environment.

An IT risk assessment requires knowledge of various aspects of the device concerned. Areas to consider include:

- The access control list (ACL) – a list of accounts and passwords (an assessment should be made of their strength) and policies (are they changed/changeable) and how they are accessible (remote/physical). Are there hard-coded (backdoor) passwords that never change? Are passwords stored as plain text or encrypted? Are there documented access levels and identities associated with each level?
- Physical access – is access to advanced features gained through a password or keypad? Is remote access to advanced features available?
- Data validation – can anyone write to memory?
- Remote access – is there a wireless card?
- Log files – are data events recorded in a file with adequate detail for later assessment (who, what, when, how)?
- Ports and services – what ports and services are used? What is the default state of unused services and ports? Can unused ports/services be disabled?
- Malware protection – is anti-virus software allowed/installed?
- Wireless and/or wired – what are the default settings? What protocol is used? How are keys managed?
- Backup – can configuration, software settings and logs be backed up and restored?
- Checksum – is there boot-up or run-time checksums used to detect changes to software?

The US Administration's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has listed some good defensive measures to protect against cybersecurity risks:

- Disconnect the device from the network, where possible. Disconnecting the affected device from the network may have operational impacts that should be considered and accounted for.
- Ensure that unused ports are closed, particularly well-known ones such as Port 20/FTP and Port 23/TELNET.
- Work with your facility's IT section to monitor and log all network traffic attempting to reach affected products via vulnerable ports.
- Use good network design practices that include network segmentation and monitor traffic passed between zones and systems to identify anomalous activity.
- Maintain layered physical and logical security to implement defence-in-depth.
- Isolate and obscure all medical devices from the internet and untrusted systems.

Note: This list is not exhaustive and consultation with cybersecurity professionals is advised.

Practice Points – Safely retaining devices

In both hospital and primary health settings, clinicians may need to safely retain contaminated sharps and medical devices to help with analysis of an adverse event

When a medical device incident occurs, clinicians are encouraged to retain devices of concern to assist with further analysis. The issue was discussed in an article in the May 2015 issue of MDSU.

If the incident involves sharps and/or medical devices contaminated with bodily fluids, it is essential that retaining the device does not place hospital staff, patients or TGA staff at further risk. It is also possible that retaining devices such as sharps can contradict occupational health and safety (OH&S) policies for individual health facilities.

A recent report to the TGA highlighted this complexity. A clinician reported that a venepuncture needle felt blunt during use with a patient and, although retaining the device was essential to assess the incident, there was no safe way to retain the contaminated sharp during the patient consultation. As a result, the needle was correctly disposed of in a wall-mounted sharps container to prevent risk to the clinician and patient.

This article aims to provide clinicians with further advice on how to safely retain devices before sending them to the TGA (if requested) or returning them to the sponsor/manufacturer for analysis.

Following a medical device incident, please submit a report to the Incident Reporting and Investigation Scheme (IRIS), retain the medical device and packaging, and wait until a representative from the TGA has contacted you to say whether the device should be sent to the TGA or the sponsor/manufacturer.

Advice for clinicians

Clinicians are advised to be alert to the following:

- Ensure that you are familiar with the relevant policies and procedures for reporting incidents with medical devices and relevant OH&S policies in your health facility.
- Determine if your health facility has a policy regarding retaining contaminated medical devices and sharps. If no policy exists, raise this with your clinical director.
- Consider having specialised containers readily available that are suitable for the types of devices used in your clinical area. For example, have small transportable sharps containers ready to access if a venepuncture device is identified as part of a device incident.
- If you need to retain a contaminated or sharp medical device, follow these steps:
  1. Ensure that you use universal precautions when handling the device and comply with OH&S procedures for your health facility.
  2. If safe to do so, clean the device as much as possible without destroying any evidence you feel contributed to the adverse event. Do not put yourself at risk of exposure.
  3. If safe to do so, contain the device in an appropriate container with hard plastic sides and a sealable lid, such as a specimen jar/bucket. Alternatively, devices can be double-packaged in plastic bags designed for transport of bio-hazardous (non-sharp) objects.
  4. Use tape to seal the container and prevent accidental removal of the lid. Use tape to seal all openings of plastics bags.
  5. Carefully label the outside of the container with the following information:
     - a description of the device
     - the number of devices within the container
     - the date
     - your name
     - ensure that the label has the words “CONTAMINATED MEDICAL DEVICE”.
     - if you have already been given a Device Incident Report (DIR) number by the TGA, please add this to the outer packaging
     - include any other details that you feel are important.
  6. Place the device in a secure area and ensure that all staff are aware of the presence of the contaminated device.
  7. Contact the relevant parties as per the policy in your health facility. This may include contacting the device sponsor/manufacturer to collect the device, and reporting the incident to the TGA.
- More information about retaining and returning medical devices for analysis can be found on this TGA webpage: Report a medical device adverse event (medical device user).

Sponsor workshops

The TGA will be conducting a series of workshops for medical device sponsors to explain their post-market roles and responsibilities

The workshops provide an opportunity for sponsors to learn about their post-market roles and responsibilities, incorporating requirements for the medical device Incident Reporting and Investigation Scheme (IRIS), annual reporting, and maintaining documentation relevant to post-market reviews (PMR).

Workshops will be held in Sydney, Brisbane and Melbourne, beginning in May 2016.

More detailed information will be emailed to sponsors and posted on the TGA website closer to the date. Further information and registrations are available by emailing iris@tga.gov.au.

Recent safety alerts

Below are TGA safety alerts relating to medical devices published since the last edition of *Medical Devices Safety Update*.

Veletri consumables kit: Recall – small risk of infection due to potential contamination

Flocare transition giving sets with ENFit transition adaptors: Recall for product correction – potential for leakage and/or breakage

HeartWare Ventricular Assist Device AC adapters and batteries: Hazard alert – potential for loss of power

Samarys polyethylethylketone anterior cervical cage: Hazard alert – potential for adverse events due to missing or protruding gold wires

What to report? Please report adverse events, as well as near misses

The TGA encourages the reporting of any suspected adverse event or potential adverse event relating to a medical device. Adverse events can involve actual harm to a patient or caregiver, or a near miss that may have resulted in harm.

Some issues relating to medical devices that may lead to adverse events and prompt you to report include:

- mechanical or material failure
- design issues
- labelling, packaging or manufacturing deficiencies
- software deficiencies
- device interactions
- user/systemic errors

Suspected adverse events or near misses can be reported directly to the TGA:

- **online** at www.tga.gov.au (click 'Report a problem')
- **by emailing** iris@tga.gov.au
- **by mail** to IRIS, TGA, PO Box 100, Woden ACT 2606
- **by fax** to 02 6203 1713

For more information about reporting, visit www.tga.gov.au or contact the TGA's Medical Devices Branch on 1800 809 361.

For the latest information from the TGA, subscribe to the TGA Safety information email list via the TGA website

For correspondence or further information about Medical Devices Safety Update, contact the TGA's Medical Devices Branch at iris@tga.gov.au or 1800 809 361

Medical Devices Safety Update is written by staff from the Medical Devices Branch

Editor:
Ms Pamela Carter

Deputy Editor:
Mr Aaron Hall

Acting TGA Principal Medical Adviser:
Dr Tony Gill

Contributors include:
Dr Cate Brogan
Dr Amanda Craig
Mr Shawn Hazel
Mr Patrick O'Meley