CMBES/SCGB
2025 CMBEC47/ACCES26
Fredericton, NB
May 27-29, 2025

# Lessons Learned from Effective Password Management for Medical Devices in Hospitals

Veronica Lu

*Veronica Lu Lower Mainland Biomedical Engineering*

## ABSTRACT

*Keywords:* Password management, hospital setting, medical device

*Conflict of Interest:* The authors declare that they have no conflict of interest.

Introduction

The growing interconnectivity of medical devices in healthcare environments has significantly heightened cybersecurity risks, leaving many devices vulnerable to unauthorized access and exploitation due to weak security features. Effective password management is crucial not only for safeguarding sensitive patient data but also for ensuring the continuous and safe operation of clinical systems (Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA) This is also gaining the attention of governing bodies, with the Office of the Auditor General in British Columbia setting out requirements for healthcare organizations, of which password management is one key recommendation.
Managing passwords in hospitals presents unique challenges due to the vast number of devices uncertainty around the current status of passwords, and variation in the appropriate selection password management tools. These challenges are compounded by limited resources, both in terms of personnel and time, making the implementation of robust protocols particularly difficult in busy healthcare environments.
This presentation outlines a practical, secure, and scalable approach to medical device password management that balances real-world usability with strong cybersecurity demands.

Methods (Approach)

Our solution, prompted by a password exposure incident, was designed to protect against cyber threats while being feasible for biomedical teams to adopt consistently.

To address the unique structure of our organization, which supports four distinct health authorities, we adopted a flexible approach. Health Authority directory logins were integrated with medical device where possible to streamline access, while centralized password management tools and two-factor authentication (2FA) were used for devices without directory support. This ensured secure password storage across all systems.

Changing password is integrated into the computerized maintenance management system work-order process, ensuring that password management tasks were clearly documented, tracked, and updated on a daily basis. Through this integration, technologists were able to promptly address issues as they arose, while also maintaining visibility and accountability across all teams involved.

Additionally, biomedical technologist were sent on dedicated cybersecurity education classes, as education was recognized as a key component to raising cybersecurity awareness and ensuring the long-term success of these protocols.

## Results

Lower Mainland Biomedical Engineering manages a total inventory of 115,001 devices, and has successfully secured 93.8% of them, leaving only 7,171 devices still requiring password management work.
This reflects the efficiency and effectiveness of our ongoing efforts to secure medical devices across the entire organization.

## Conclusions

This presentation emphasizes the importance of establishing effective communication with technologists to manage unknown password statuses across large inventories, all within the constraints of available resources. Real-world examples demonstrate how these solutions have improved device security, ensured compliance with Office of the Auditor General of B.C. recommendations, and minimized operational disruptions. By achieving a balance between protection and practicality, this approach offers hospitals a viable pathway to enhanced cyber-security.