imprivata®

Welch Allyn®

Best practices: Access controls for medical devices

Who should read this

- **IT executives** concerned about the security of medical device access
- **IT professionals** looking to ensure data integrity in the EHR
- **Clinical informatics leaders** looking to align clinical workflows and data security requirements
- **Anyone** concerned about securing PHI

Executive summary

- Concerns around cybersecurity threats in today's healthcare IT environment are cause for careful consideration when evaluating network-capable devices and solutions
- Medical devices used by frontline caregivers and connected to an institution's HIS infrastructure can offer benefits including improved clinical user efficiency, as well as enhanced timeliness and accuracy of patient information
- Understanding the opportunities and options for implementation of solutions that are both secure and offer high clinical usability should be an important aspect of the technology evaluation process for connected medical devices

In this paper, we'll offer insights on key challenges, considerations, technologies, and workflows related to providing secure frontline medical device access and use.

Introduction

Healthcare information technology has quickly become one of a clinician's most powerful instruments. The implementation of technology to automate the collection and documentation of patient information, such as vital signs, continues to expand to users in more care settings within the hospital environment. Robust, network-capable devices, in these cases, are distributed and often mobile in nature and come with the ability to not only read a patient's vitals, but also capture that information, store it, aggregate it, and transmit it to other networks, devices, and applications within the healthcare IT infrastructure – namely the institution's EHR system. The result is a complex partnership between people, information, and technology which ultimately supports the delivery of high-quality patient care. However, interconnectivity can raise security and compliance considerations. In order to help ensure safety, organizations must be able to trust the exchange of information that is facilitated through these medical devices.

Traditional means of securing these devices and ensuring proper compliance can inhibit provider productivity and cause frustration for users. For this reason, the burden of security falls into many hands: those of device manufacturers, healthcare organizations, providers, and even patients.

As a first step, many device manufacturers have started to implement changes that will allow for easier risk management and mitigation, including access controls. However, healthcare organizations must understand how to best manage these new security measures in order to help ensure user compliance and avoid disruption to clinical workflows.

While the topic of medical device security seems to be top of mind for the entire healthcare industry, regulators have yet to weigh in on the best approach. A successful medical device security strategy must include best practices for implementing access controls on medical devices to help increase security and ensure compliance without impeding patient care.

Considerations and recommendations from regulators

Over the past several years, the FDA has released guidance and recommendations to align medical device manufacturing processes with cybersecurity best practices. This guidance encourages manufacturers to design medical devices with cybersecurity in mind to aid in the prevention and mitigation of threats once a device has been deployed within a healthcare environment. From the FDA's standpoint, as well as that of manufacturers and healthcare providers, the largest concern when it comes to medical device cybersecurity is ensuring that cyber threats do not impede device functionality and, thus, patient safety. One of the primary methods for security outlined in the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices is to prohibit untrusted users from gaining access to these devices by enabling strong authentication. In response, many medical device manufacturers have designed configurable access controls such as the use of username and password to help ensure that only trusted users can gain access to networked medical devices and the sensitive PHI with which they interact. These access controls help align medical devices more tightly with the National Institute of Standards and Technology (NIST)'s cybersecurity best practices for protection, detection, and remediation.

Similarly, the Health Care Industry Cybersecurity Task Force's June 2017 publication, Report on Improving Cybersecurity in the Health Care Industry, leverages the NIST Cybersecurity Framework to identify areas of focus to help improve medical device security and privacy for both manufacturers and healthcare providers. While the NIST best practices have long been standard practice throughout the information technology arena, it is just recently that organizations have been forced to apply the same techniques to medical devices. Unfortunately, many standard security best practices are not yet practical or effective for medical devices. While the industry quickly moves to better address these concerns, the Cybersecurity Task Force has outlined steps that organizations can take now to address primary trust concerns for medical devices. In recommendation 2.4 of the report, the task force suggests that organizations "require strong authentication to improve identity and access management for health care workers, patients, and medical devices/ EHRs" (NIST, 2017) .

More specifically, they suggest the use of single- or two-factor authentication to better establish trust between clinicians and devices, as well as between the devices and the networks with which they communicate PHI.

Many medical device manufacturers have designed configurable access controls to help ensure that only trusted users can gain access to networked medical devices and the sensitive PHI with which they interact.

In order to have a successful access control strategy for medical devices, healthcare organizations must plan for some of the most common workarounds that are seen in healthcare today.

Following these practices can help to mitigate some of the most prevalent risks facing network-connected medical devices today, including access by malicious or untrusted users, tampering with patient health information, data integrity concerns as information is shared between devices and EHRs, exposure of PHI knowingly or inadvertently on unlocked devices, and even patient safety issues on devices that support clinical decision-making and the delivery of care. Access control, through the use of strong single- or multifactor authentication, can play a key role in threat protection and identification as it allows organizations to lock down devices and bring an added point of visibility and auditability during clinical workflows – so long as these controls do not interfere with provider productivity or the delivery of patient care.

Understanding common security and compliance workarounds

Too often, increased security measures can contribute to a decline in provider efficiency, productivity, and satisfaction. Introducing additional workflows or cumbersome tasks in the name of security can often have unintended impacts, as clinicians and other users employ workarounds to mitigate frustration associated with new security measures. For some medical devices, such as patient spot check vitals monitors, clinicians may have to log in to access the device multiple times per shift. In order to have a successful access control strategy for medical devices, healthcare organizations must plan for some of the most common workarounds that are seen in healthcare today.

Not requiring credentials

The security and compliance risks of not requiring credentials for network-connected medical devices, or for those that store PHI, are limitless. The risks range anywhere from a HIPAA fine when a patient monitor is left unattended, to an entire network compromise as a networked device is used as a backdoor entry to the HIT infrastructure, or even patient safety concerns in the event an untrusted user pushes incorrect information to the EHR, compromising the integrity of a device's clinical decision-making support.

Password and credential sharing, leading to audit Issues

When clinicians are required to manually enter usernames and passwords, they often resort to unsecure activities, such as the sharing of user credentials to remove some of their workflow pain points. This can be done in the form of password sharing between clinicians or in the form of clinicians opting to stay logged in to the devices, creating the potential for inadvertent charting under the incorrect clinician ID. Not only does this activity expose organizations to the risk that an untrusted user can gain access to one of these medical devices, it also interferes with data accuracy as audit logs can no longer be trusted.

Batch entry and hand written vitals
To optimize the investment in vital signs monitors that can connect in a secure way, hospitals have to configure devices to authenticate clinicians. If the process is viewed as one that creates inefficiency and frustration with the clinical staff, the hospitals may configure for less security than is desirable, or see low adoption of the technology with manually charted vitals.

Not connecting devices to the network
Occasionally, in an attempt to avoid common security frustrations, organizations will keep these medical devices off of the network. While this may remove some of the most common security concerns, it also prevents healthcare organizations from optimizing the investments they have already made in their connectable medical devices.

By ensuring that access controls on medical devices are streamlined, convenient, and do not interfere with clinical workflows, organizations can avoid dangerous security workarounds before they happen.

Evaluating authentication modalities for the care setting

Undoubtedly, the best way to help ensure security and compliance is to map out an access control strategy that is specifically tailored to the unique needs of the healthcare environment. While NIST, the FDA, and the Cybersecurity Task Force recognize many authentication modalities as approved and secure, not all of them make sense at the point of care.

Workflow considerations
When selecting an authentication modality or workflow, it's important to understand the care setting in which the authentication will happen. For example, FIPS-compliant biometric authentication may make sense in some areas of the hospital, such as shared workstations or nurse stations, but may not be as practical in care settings where gloves are required. Similarly, while proximity cards are convenient and easily accessible during regular patient interactions, they may not be the best approach in operating rooms. Therefore, flexible authentication that gives the user the option of more than one modality can help account for varying scenarios.

Single-factor vs. two-factor authentication
Another factor to take into consideration during evaluation of an access control strategy is when and where to employ single-factor authentication and two-factor authentication. The FDA stresses the importance of ensuring that authentication not interfere with patient care. It's important to consider what level of security is required and practical for each situation. Some workflows, such as transmitting blood pressure or temperature readings, may only require one level of security, whereas other workflows may require multiple factors, either due to internal mandates or government regulations (e.g., medication dispensing in certain states). Consult with both clinical and compliance teams to understand which option makes the most sense for your medical devices and care settings.

Tip: Use audit logs during a brief discovery period to gather a baseline for clinician interaction with devices. This data can help better align grace periods with actual clinical workflows.

Tip: Start sessions short and increase over time if they are found to be burdensome. It's always easier to extend a grace period than shorten one.

For further information please contact us at
1 781 674 2700
or visit us online at
www.imprivata.com

Offices in
Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

Grace periods

One of the largest roadblocks to access control compliance is the burden put on clinicians to repeatedly enter user credentials throughout the day. Consider implementing grace periods to further streamline authentication once a user has established trust.

In selecting the proper timeframe for a grace period for a medical device, it's imperative to understand how clinicians are using each device in the field.

A grace period for one type of device, such as a spot check vitals monitor, may need to be different than that for an infusion pump or other medical device.

Break-glass considerations

Consider multiple modality options to ensure that trusted clinicians can access devices through various methods in the event that one is not available. For example, a patient vitals monitor may be configured to accept a proximity badge for a trusted user as well as the manual entry of username and password in the event a clinician does not have his or her badge. Additionally, a vitals monitor may be configured to only transmit data after authentication, but still allow for vitals to be taken to quickly asses any immediate patient health concerns.

Bringing access controls to your medical devices

Imprivata, the healthcare IT security company, and Welch Allyn, a leading global provider of medical diagnostic equipment, have partnered to enhance the security of medical devices through streamlined access control. The Imprivata-Welch Allyn collaboration extends the Imprivata Confirm ID™ for Medical Devices platform into the Welch Allyn Connex® vital signs portfolio. By enabling fast, secure authentication for accessing and transacting with patient information on medical devices, security and auditing capabilities can be improved without compromising clinician efficiency and patient care. For clinicians, this means a faster, more efficient login to the device, helping them to focus on their primary business of patient care.

1. FDA, October 2014, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
2. NIST: National Institute of Standards and Technology
3. Health Care Industry Cybersecurity Task Force, June 2017, *Report on Improving Cybersecurity in the Health Care Industry*, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
4. NIST, June 2017, NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Life Cycle Management*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

CID-WP-MD-0218