DEVICE AUTHORITY

SECURING IOT MEDICAL DEVICES

A guide for device manufacturers and medical professionals

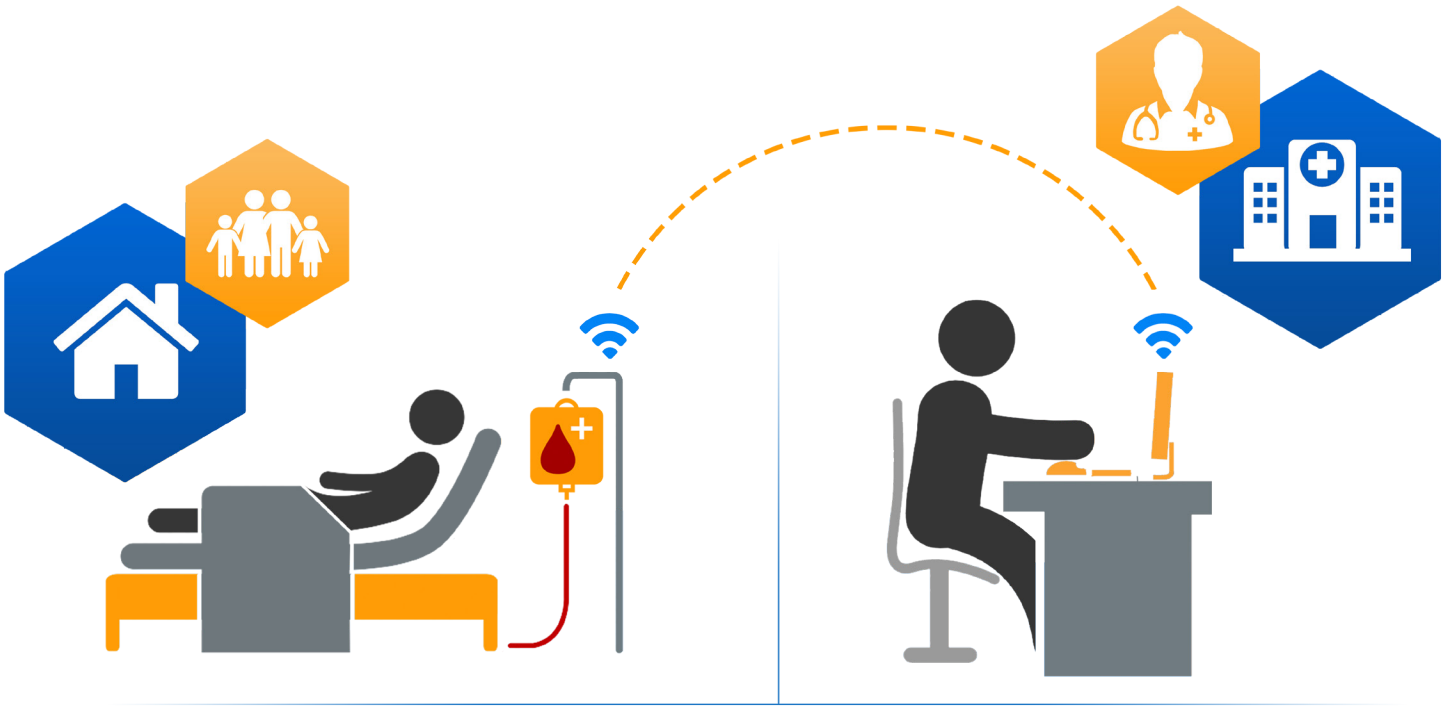
Abstract

Experts predicted that like the Internet, the Internet of Things (IoT) too is going to be a part of our everyday life. With an increasing number of medical devices connecting to the Internet, the idea of a connected healthcare sphere becomes more interesting. Several software, service, and product companies are showing interest in connecting devices with a view to make their primary product or service more achievable.

IoT devices provide many benefits for different stakeholders, most notably improved healthcare for patients, efficiency and cost savings for the manufacturer and real time monitoring for healthcare professionals. However, there are risks associated with connecting medical devices to the Internet. The good news is there are ways to mitigate them, which will be addressed in this guide.

This guide provides an overview of connected or IoT medical devices, their benefits and risks, real life use cases and best practice security guidelines.

For more information, please contact Device Authority.



Introduction

What is a Connected Medical Device?

Simply defined, a connected medical device is:

- Connected to the Internet
- Transmits data
- Wired or wireless

What are the Benefits of Connected Medical Devices?

The healthcare industry benefits tremendously from the Internet of Things (IoT). Here are some key benefits:

Real-time monitoring and data

Medical devices can transmit dynamic data from a patient home to hospital staff. It allows healthcare professionals to have real-time monitoring of patient's health. This continuous patient monitoring produces real-time analytics and alerts when there are fluctuations in patients' vital statistics. Real-time monitoring captures early warning signs of health problems and collects health-related "big data".

Enhanced patient care

Connected medical devices encourage improved coordination and delivery of patient care through a 360* view of patient and the disease, improving the effectiveness of treatment plan;

- Compliance with dosing schedule
- Maintaining accurate records of dosing, monitoring

Efficiency and cost savings for manufacturer

The device manufacturer or supplier can also utilise real-time monitoring to observe device performance.

What are the Key Concerns or Risks of Connected Medical Devices?

There are huge benefits of connected devices, but of course there are also concerns and risks associated with connecting medical devices to the Internet.

Standards / Compliance

- Legal

Security and Privacy

- Patient health and safety
- Loss of PHI / data
- Network attacks

Interoperability

Cost

Reputational

Connecting devices, people, and systems has particularly strong impacts in the healthcare industry. Up-to-the-second information can mean the difference between life and death for patients, and the potential applications of connected technology to improve care are endless. Pacemakers that doctors can remotely monitor and maintain to identify problems before a heart attack and insulin pumps that can be adjusted wirelessly, giving a patient more control and better care are already a reality.

As in the digitization of any industry, the same connectivity that drives significant value simultaneously heightens security and privacy risks. The main threats fall in two categories:

Personal Data Theft

Hackers can access medical and financial information through IoT devices.

Vulnerabilities in a networked medical device pose obvious privacy risks, since these devices access patients' most personal biological data. Hackers may use connected medical devices to steal patients' data for identity theft, targeted blackmailing, buying drugs or medical equipment to resell and filing fraudulent insurance claims. Additionally, if these devices interface with medical billing records, then patients risk losing both medical and financial information.

Intentional Disruption and Device Tampering

Cyber terrorists can close entire hospital systems and immobilize services.

Intentional disruption and cyber terrorism pose significant risks, because networked medical devices face the same technological vulnerabilities as any other networked technology. Security vulnerabilities have been discovered in pacemakers, defibrillators, and diabetes insulin pumps. These devices are meant to be communicating with the management server only, but have been found to broadcast signals out into the Internet, breaching security protocols.

To cite an example, Johnson & Johnson's insulin pump turned out to be highly vulnerable due to the unencrypted wireless connection between the remote and the pump, giving hackers a chance to easily implement their malicious techniques: to trigger unauthorised insulin injections and access the entire hospital system to immobilise services and cause panic and chaos.

As the worlds of healthcare, wireless connectivity and mobile devices collide, security of the data/information transmitted needs to be carefully considered. The data being transmitted can vary from very low risk to very high risk, and the means of device design to secure data and authenticate devices must be considered.

To ensure the safety of patient data, the FDA released a new draft guidance that addresses the steps manufacturers must follow in order to protect medical devices against cyberattacks.

Examples of IoT Medical Devices

Wearables

Home health monitoring devices

- Insulin pump
- Defibrillators
- Cardiac monitors

Surgical robots

Real-time monitoring

- ICU procedure

Wearable devices and home health monitoring devices assisting patients is a common thing now. Chatty medical devices are extremely appealing for patients of any age range. As IoT continues to become an integral part of our everyday lives, the opportunity to use it within device applications remains promising.

Who is Responsible for Security?

As the worlds of healthcare, wireless connectivity and mobile devices collide, security of the data/ information transmitted needs to be carefully considered. The data being transmitted can vary from very low risk to very high risk, and the means of device design to secure data and authenticate devices must be considered.

To ensure the safety of patient data, the FDA released a new draft guidance that addresses the steps manufacturers must follow in order to protect medical devices against cyberattacks.

Device manufacturers and OEM / chip makers and device designers must identify, investigate and overcome these challenges so that the implementation of smart connected medical technologies can be achieved.

Healthcare providers and device manufacturers should share the responsibility.

Cybersecurity throughout device lifecycle

"Manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device."

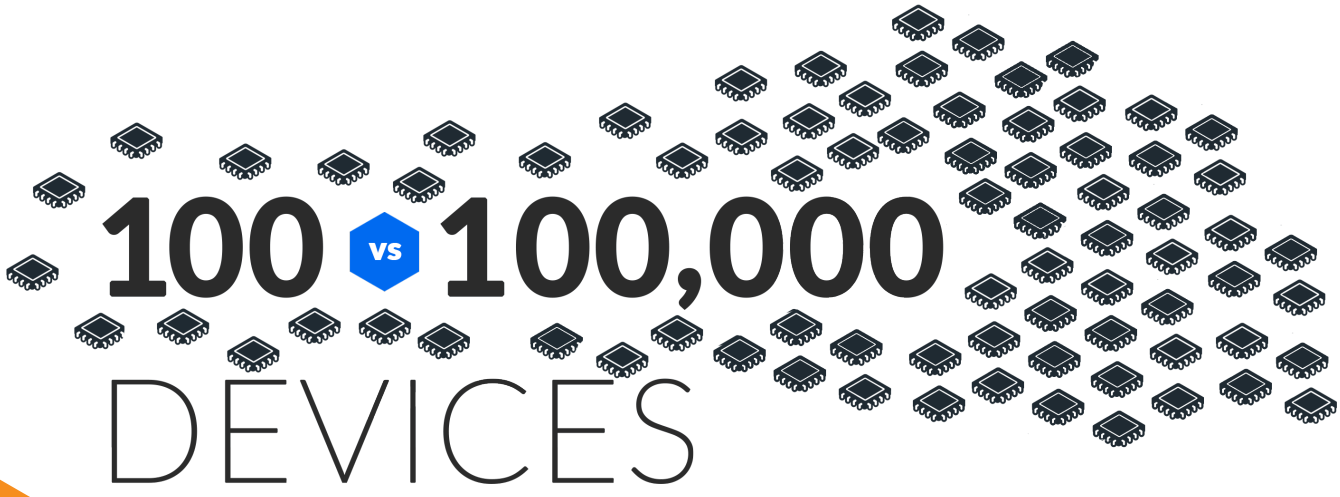
Source: Postmarket Management of Cybersecurity in Medical Devices, FDA, Dec. 2016

Common Security Challenges

Provisioning & managing device identities at scale

- Creating scalable, distributed trust requires sophisticated PKI implementation

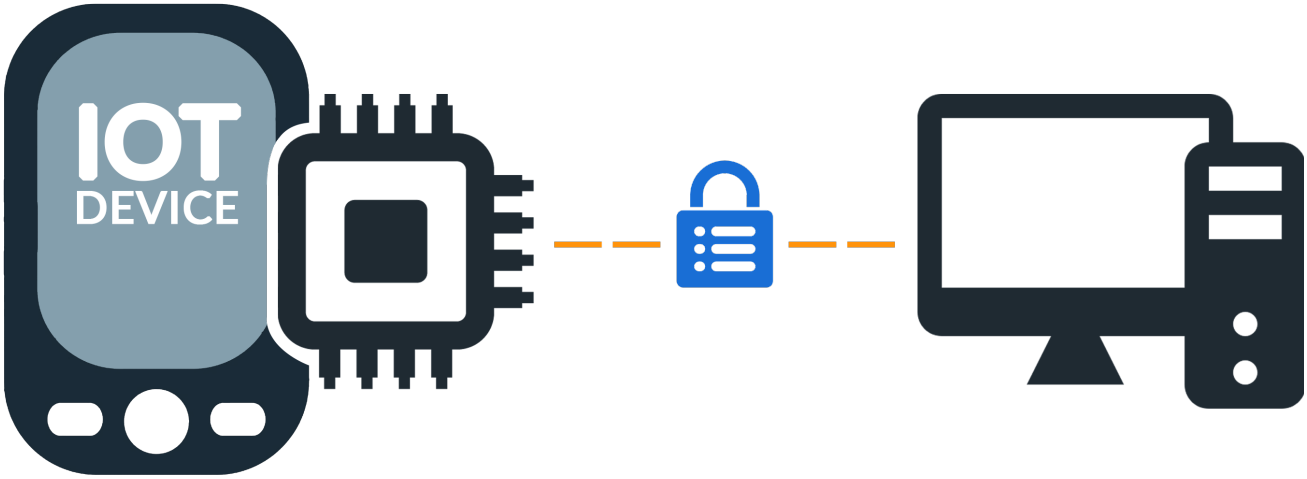
"Managing 10 devices is easy, managing 10,000 is hard!"



Implementing the correct data protection controls

- Ensuring only authorized entities have access to sensitive data

"Encryption is easy, managing keys is hard!"



Preventing unauthorized access to devices

- Ensuring all updates and data sent to device are locally verifiable

"Controlling access to server resources is easy, doing the same on the device is hard!"

Identify Risks and Security gaps

Assess device capabilities and consider the exploitation points

- Does the device use WIFI or Bluetooth?
- Is there a remote access service? (e.g. SSH)
- Can peripherals be plugged in? (e.g. USB, Network port)
- Is the disk accessible/removable? (e.g. SD Card)

Evaluate data security requirements

- Does the device send/receive sensitive data?
- Can sensitive data be exported from the device?

Determine if device-to-device trust is required

- Will this device communicate with other local devices?

Implement mechanisms to provide software security updates

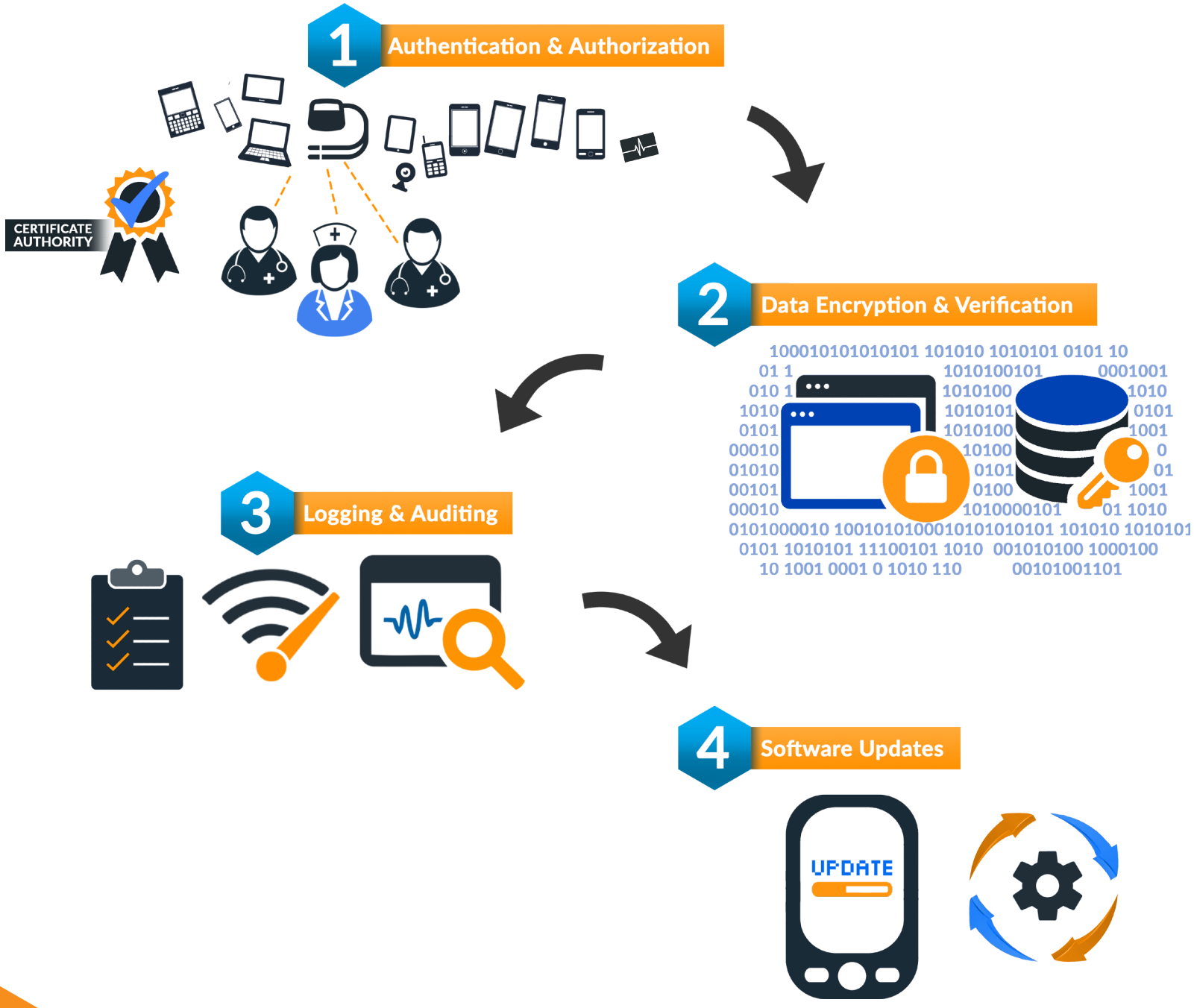
- FDA does not necessarily require re-approval for “routine security updates”

  https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

How to Secure a Connected / IoT Medical Device

At the foundation of security for medical devices is two key areas:

1. Device Identity and integrity (device authentication and authorization)
2. Data security and privacy (data encryption and verification)



Authentication and Authorization

Avoid hardcoded or common credentials

- Every device should have unique credentials

Provision identities that can be cryptographically validated

- Use a Public or Private Root Certificate Authority to issue device certificates
- Leverage a TPM in devices to secure keys in hardware, where appropriate
- Use HSMs with server-side applications to prevent unauthorized access

Authenticate and authorize DEVICES

- When accessing server resources
- When communicating with other local devices or systems

Authenticate and authorize USERS

- Use multi-factor authentication for user access (e.g. System admins, service personnel)
- Ensure users are authenticated when accessing devices

Data Encryption and Verification

Maintaining the privacy of patient records and data is paramount to healthcare. If a healthcare facility or device collects patient data and exchanges this data over the internet, then data privacy and security is a real problem. Strong IoT security is critical to prevent hacking and data breaches. **A security breach is not just data loss, it is the safety (life in danger) issue**.

Secure data flowing to and from devices using standardized crypto methods

- e.g. NIST-approved AES256

Cryptographically sign data to protect against tampering in transit

- Use device-unique asymmetric keys to provide evidence of source
- Store private key in device TPM

Centralize controlled access to sensitive data

- Couple user and device authentication with authorization policies to control access to data and crypto keys

Encrypt sensitive data at rest

- Secure data that resides on both the device, and on servers

Logging and Auditing

Log all security actions for auditing purposes

Create a digital “paper trail” to keep visibility of important security actions

- Who is your device talking to?
- Who is accessing the sensitive data?
- Did this data come from a verified source?

Detect, notify, and remediate security concerns

- Failed authentications
- Unauthorized access to resources
- Device tampering

Software Updates

Implement a SECURE software update mechanism

- Cryptographically sign all software updates
- Perform proper signature validation against update files on device before executing
- Ensure secure transfer of update data to device

Require user/device authentication before applying software updates

Follow software update guidelines from the appropriate regulatory body

- The FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity

Routine Updates and Patches

"The majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits, referred to as "cybersecurity routine updates and patches," are generally considered to be a type of device enhancement for which the FDA does not require advance notification or reporting."

Source: Postmarket Management of Cybersecurity in Medical Devices, FDA, Dec. 2016

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

Compliance

EU GDPR - General Data Protection Regulation

Security Breaches

A major privacy concern for IoT devices is hackers and security breaches. The GDPR introduces a mandatory notification; personal data breaches must be reported within 72 hours.

Consent

There is doubt whether IoT devices obtain quality consent from users in relation to the processing of data. The GDPR requires data controllers to show consent has been given by way of a clear positive act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data.

Privacy by design and privacy by default

The GDPR will put these two concepts on firm legislative footing. Organizations must adopt significant technical and organizational measures to demonstrate compliance with the GDPR, and conduct data protection impact assessments.

Enhanced data subject rights

An express right to be forgotten, data portability rights, and the right to object to automated decision making are all included. This is important for the design of IoT devices as the necessary capabilities must be built from the start.

Processing personal data relating to children

The GDPR makes it impossible for children aged 12 and under to consent on their own behalf

HIPAA - Health Insurance Portability & Accountability Act

Sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that the required physical, network, and process security measures are in place and followed.

Implement a security solution which provides end-to-end data encryption for PHI data, both at rest and while it is in transit. Leveraging AES 256 and other widely adopted standards, end-to-end encryption is not only considered a Safe Harbor to the HIPAA regulations but also provides a way to dynamically authenticate devices which helps eliminates the overhead and costs typically associated with managing keys and certificates.

Conclusion

When designing a connected medical device, always consider security and privacy from the beginning – at the design stage ideally. In a rush to innovate and get to market quickly, security can often be overlooked. However, in a sensitive, regulated healthcare environment it's crucial to get security right.

Start by considering the threats, and then evaluate secure solutions to overcome them.

Hopefully this guide has provided you with a good grounding in security for connected medical devices.

Please note we can also support offline devices.

Should you require deeper technical knowledge, or would like to speak with someone, we're the experts ready to advise, please contact Device Authority.

Our Vision:
"To secure and provision applications, data and devices without human intervention"

Trust for every Thing

Device Authority provides solutions to address the challenges of Identity and Access Management for the Internet of Things (IoT) without human intervention. We help our customers and partners simplify the process of establishing trust for the IoT, enabling end-to-end security architecture and scale for the IoT through our innovative technology platform.

IoT brings new security challenges introduced by the scale and pace of adoption, as well as the physical consequences of compromised security. These challenges cannot be effectively addressed by traditional Information Technology (IT) security solutions. The KeyScaler platform is purpose-built to address these challenges through automated device provisioning, credential management and policy-driven data encryption.

With offices in Fremont, California and Bracknell, UK, Device Authority partners with the leading IoT ecosystem providers, including Amazon Web Services (AWS), Comodo, Thales, Dell, Intel, PTC and DigiCert (Symantec). Keep updated by visiting www.deviceauthority.com and following @DeviceAuthority on Twitter.

Version 1 - Written by Rosa Lenders and James Penney

sales@deviceauthority.com

www.deviceauthority.com

© 2018 Device Authority. All rights reserved.

UK Head Office
2 Arlington Square,
Venture House,
Downshire Way,
Bracknell, RG12 1WA

North America Office
39300 Civic Center Drive,
Suite 180,
Fremont, CA 94538
USA