hsd Best Practices


# Cybersecurity in Medical Devices through Full Systems Design Strategies

**Jon Steer** | Director of Software

Smart networked medical devices are on the rise, therefore demanding increased cybersecurity and closer adherence to modern cybersecurity regulatory guidelines. This white paper focuses on:

- Security in the era of smart networked medical devices
- Designing medical devices with a multidisciplinary team
- Examples of proactive security activities
- Security steps for a device's life-cycle
- Main types of exploits and how to prevent attacks

## Security in the Era of Smart Networked Medical Devices

With the advent of smart networked medical devices, addressing cybersecurity regulatory demands has become a major design task for medical device manufacturers. Protecting the device from cybercriminals, who are not just after personal data, but who are also after intellectual property such as in the Community Health Systems breach, requires approaching the design from multiple security angles. Cybersecurity puts pressure on new medical device designs to solve these problems at the system architecture and design stage of the product lifecycle.

The days of a medical device performing a simple task in isolation have long gone. With ever-higher levels of enterprise integration such as equipment tracking, lab management, medical record generation and mobile devices, security for a medical device needs to be addressed in every system discipline and cannot be an afterthought.

*Cybersecurity puts pressure on new medical device designs to solve these problems at the system architecture and design stage of the product lifecycle.*

Cybersecurity must be part of any risk analysis for the device. Although the FDA has not formally mandated cybersecurity, they clarified their thoughts in a non-binding Guidance document titled **"Content of Premarket Submissions for Management of Cybersecurity in Medical Devices"** in Oct of 2014.

## Cross-Discipline Team

Having a cross-discipline team consisting of Research, Industrial Design, User Experience, Electrical, Mechanical, Systems and Software Engineering working closely together is more imperative than ever. Integration of all disciplines will lead to problem solving early in the design stage resulting in considerably quicker time to market, reduced development costs and more stringent security controls.

*Integration of all disciplines will lead to problem solving early in the design stage resulting in considerably quicker time to market, reduced development costs and more stringent security controls.*

---

**Examples of Proactive Security Activities should Include:**

- The Software team reviewing, auditing and testing the code continuously for security holes and backdoors.
- The UX team reducing friction points and creating an easy to use, intuitive, integration setup and authentication system.
- The EE team using processor designs that include encryption engines and block locking flash memory.
- The ME team designing interlocks and tamper indicators into the enclosure.

## Proactive Security Steps for a Device's Lifecycle

**Proactive steps could include:**

- **Requirements** | making cybersecurity a "must have" and present at the minimum viable product stage
- **Design** | having third party security reviews of design and architectural components.
- **Development** | using virtual machines to run security audits in addition to continuous system builds
- **Unit and System Testing** | adding secure logging facilities into designs
- **Verification and Validation** | run fuzzing attacks on the device during security audits
- **Deployment** | setup Two Factor authentication for maintenance personnel and give customers clear security directions
- **Updating** | fast, secure deployment strategies to deal with "zero-day" exploits such as "HeartBleed" in a timely fashion
- **Retirement** | ways to completely scrub the system, not just "set to factory default"

## Guarding Against Exploits

**There are three main types of exploits**

1. Physical - the attacker has physical access to the device and can access components
2. Network Based - The attacker must exploit some network facing component of your system
3. Social Engineering - The attacker exploits some organizational fault, such as weak passwords, third party tech support

Physical attack prevention will require some changes in traditional device architecture, for example, “USB sneaker net”, whereby USB keys are used for transferring information. As has been reported, there are a number of new hardware attacks using USB keys that are undetectable by normal means.

**Thwarting network attacks may involve multiple approaches, such as:**

- Reducing the network access to/from the device using PANs (Personal Area Network) technology such as 6LOWPAN
- Using mesh networks to separate the processing, display and storage with decomposed, multi-processor, multi-node designs.
- Generating custom operating systems that get rid of excess software dependencies and reduce the “attack surface” of the system.

Social Engineering attacks always start at the places of most user friction. For example, the onboard keyboard is painful and slow, so, easy three letter passwords are used. Preventing social engineering exploits is where UX/UI adds great value to the security process. When removing password-based authentication and substituting physical forms of authentication, making authentication as frictionless as possible becomes a priority task for UX design.

UX design should pay particular attention to setup and configuration of the device so that hurried IT administrators will not be tempted to take shortcuts when setting things up. Reducing the number of interdependent system options so that the users are not just taking the default is another way to be sure that the system stays secure.

***When removing password-based authentication and substituting physical forms of authentication, making authentication as frictionless as possible becomes a priority task for UX design.***

In the end, designing medical devices and lab instruments that have many-year lifespans and that can withstand exploits that have yet to be discovered will require system designs to apply new methodology.

## Be Prepared

Traditional approaches like "we'll get around to it in the next release" will not result in products that will pass either customer security audits or regulatory scrutiny. These approaches, although appear like a quick to market solution, can lead to costly impacts on time and money.


HS Design is a user centered design firm specializing in Medical and Scientific products and delivery systems. At HS Design, we integrate our insight, experience, and innovation with user needs and client core competencies to develop products that exhibit a strategic advantage in the marketplace. Our combination of Research, Industrial Design, User Interface, Mechanical, Electrical and Software Engineering allows us to design for diverse environments. Our implementation to manufacturing makes it a reality.

HS Design (HSD) is an ISO 13485 & ISO 9001 certified firm with a focus on FDA compliance. At HSD we are constantly improving the value and integrity of our products and services, with an unparalleled commitment to quality. Our ISO certifications align our management system to the FDA's Quality System Regulation requirements, while meeting the globally recognized ISO requirements for the design and development of medical products. Additionally HSD is a member of the Association for the Advancement of Medical Instrumentation (AAMI) Human Factors Committee.

**Our commitment to excellence and strong relationships with our client partners has yielded over a dozen Medical Device Excellence, Consumer Innovation and Industrial Design Awards.**

**CONTACT US**

HS Design, Inc.
17 Mendham Road
Gladstone, NJ 07934

908.234.2331
info@hs-design.com

**www.hs-design.com**