EVALUATION OF MEDICAL DEVICES

Validation and verification

Main article: Validation and verification (medical devices)

Validation and verification of medical devices ensure that they fulfil their intended purpose. Validation or verification is generally needed when a health facility acquires a new device to perform medical tests.The main difference between the two is that validation is focused on ensuring that the device meets the needs and requirements of its intended users and the intended use environment, whereas verification is focused on ensuring that the device meets its specified design requirements.

Medical device manufacturing requires a level of process control according to the classification of the device. Higher risk; more controls. When in the initial R&D phase, manufacturers are now beginning to design for manufacturability. This means products can be more precision-engineered to for production to result in shorter lead times, tighter tolerances and more advanced specifications and prototypes. The arrival of CAD and other modelling platforms accelerated this process, acting both as a tool for strategic design generation and marketing.

Failure to meet cost targets will lead to substantial losses for an organisation. In addition, with global competition, the R&D of new devices is not just a necessity, it is an imperative for medical device manufacturers. The realisation of a new design can be very costly, especially with the shorter product life cycle. As technology advances, there is typically a level of quality, safety and reliability that increases exponentially with time.[68]

For example, initial models of the artificial cardiac pacemaker were external support devices that transmits pulses of electricity to the heart muscles via electrode leads on the chest. The electrodes contact the heart directly through the chest, allowing stimulation pulses to pass through the body. Recipients of this typically developed an infection at the entrance of the electrodes, which led to the subsequent trial of the first internal pacemaker, with electrodes attached to the myocardium by thoracotomy. Future developments led to the isotope-power source that would last for the lifespan of the patient.

Software

Main article: Medical software

Mobile medical applications

With the rise of smartphone usage in the medical space, in 2013, the FDA issued to regulate mobile medical applications and protect users from their unintended use, soon followed by European and other regulatory agencies. This guidance distinguishes the apps subjected to regulation based on the marketing claims of the apps. Incorporation of the guidelines during the development phase of such apps can be considered as developing a medical device; the regulations have to adapt and propositions for expedite approval may be required due to the nature of 'versions' of mobile application development.

On September 25, 2013, the FDA released a draft guidance document for regulation of mobile medical applications, to clarify what kind of mobile apps related to health would not be regulated, and which would be.

Cybersecurity

Further information: Medical device hijack

Medical devices such as pacemakers, insulin pumps, operating room monitors, defibrillators, and surgical instruments, including deep-brain stimulators, can incorporate the ability to transmit vital health information from a patient's body to medical professionals. Some of these devices can be remotely controlled. This has engendered concern about privacy and security issues, human error, and technical glitches with this technology. While only a few studies have looked at the susceptibility of medical devices to hacking, there is a risk. In 2008, computer scientists proved that pacemakers and defibrillators can be hacked wirelessly via radio hardware, an antenna, and a personal computer. These researchers showed they could shut down a combination heart defibrillator and pacemaker and reprogram it to deliver potentially lethal shocks or run out its battery. Jay Radcliff, a security researcher interested in the security of medical devices, raised fears about the safety of these devices. He shared his concerns at the Black Hat security conference. Radcliff fears that the devices are vulnerable and has found that a lethal attack is possible against those with insulin pumps and glucose monitors. Some medical device makers downplay the threat from such attacks and argue that the demonstrated attacks have been performed by skilled security researchers and are unlikely to occur in the real world. At the same time, other makers have asked software security experts to investigate the safety of their devices. In June 2011, security experts showed that by using readily available hardware and a user manual, a scientist could tap into the information on the system of a wireless insulin pump in combination with a glucose monitor. With the PIN of the device, the scientist could wirelessly control the dosage of the insulin. Anand Raghunathan, a researcher in this study, explains that medical devices are getting smaller and lighter so that they can be easily worn. The downside is that additional security features would put an extra strain on the battery and size and drive-up prices. Dr. William Maisel offered some thoughts on the motivation to engage in this activity. Motivation to do this hacking might include acquisition of private information for financial gain or competitive advantage; damage to a device manufacturer's reputation; sabotage; intent to inflict financial or personal injury or just satisfaction for the attacker. Researchers suggest a few safeguards. One would be to use rolling codes. Another solution is to use a technology called "body-coupled communication" that uses the human skin as a wave guide for wireless communication. On 28 December 2016, the US Food and Drug Administration released its recommendations that are not legally enforceable for how medical device manufacturers should maintain the security of Internet-connected devices.

Similar to hazards, cybersecurity threats and vulnerabilities cannot be eliminated but must be managed and reduced to a reasonable level. When designing medical devices, the tier of cybersecurity risk should be determined early in the process in order to establish a cybersecurity vulnerability and management approach (including a set of cybersecurity design controls). The medical device design approach employed should be consistent with the NIST Cybersecurity Framework for managing cybersecurity-related risks.In August 2013, the FDA released over 20 regulations aiming to improve the security of data in medical devices, in response to the growing risks of limited cybersecurity.

Artificial intelligence

Main article: Artificial intelligence in healthcare

The number of approved medical devices using artificial intelligence or machine learning (AI/ML) is increasing. As of 2020, there were several hundred AI/ML medical devices approved by the US FDA or CE-marked devices in Europe. Most AI/ML devices focus upon radiology. As of 2020, there was no specific regulatory pathway for AI/ML-based medical devices in the US or Europe. However, in January 2021, the FDA published a proposed regulatory framework for AI/ML-based software, and the EU medical device regulation which replaces the EU Medical Device Directive in May 2021, defines regulatory requirements for medical devices, including AI/ML software. In January 2025, the FDA published a draft guidance document for AI-enabled medical devices, covering both lifecycle considerations and marketing submissions.