Cybersecurity of medical devices

Addressing patient safety and the security of patient health information

Richard Piggin, Security Consultant, Atkins

bsi.

Contents

List of figures

Introduction

Increasing connectivity of medical devices to computer networks and the convergence of technologies has exposed vulnerable devices and software applications to incidents. The need to protect patient data from cyber-attack is now well understood. However, the potential impact on clinical care and patient safety is raising concerns for healthcare organizations, regulators and medical device manufacturers alike. Control of a medical device could also be compromised.

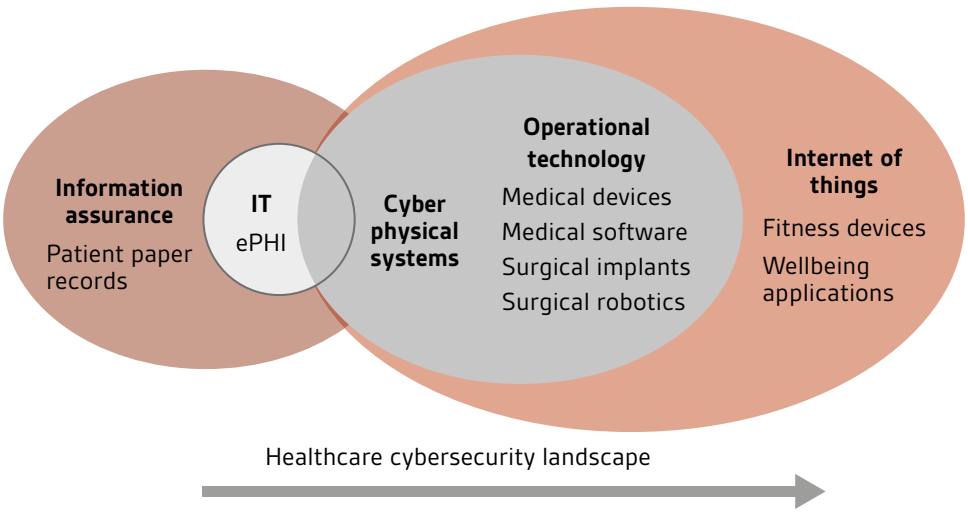
This paper considers the cybersecurity challenges facing the healthcare sector arising from the convergence of technology, hyper-connectivity and recent developments in regulation. It explains the issues and tensions between safety and security and what can be done to resolve them. The paper highlights emerging good practice and approaches that manufacturers can take to improve medical device security throughout its lifecycle. The paper will also be of interest to others in the sector, including healthcare providers, IT suppliers, notified bodies and regulators. They will recognize the requirement to address security explicitly throughout the product/system lifecycle, including design, procurement, monitoring/auditing and during operation, particularly when the inevitable cyber incident occurs.

There has been exponential growth in types of medical devices, often connected to smart devices such as mobile phones, tablet computers and wearable devices, which also run medical applications/software. These devices are already found in homes today. The inherent security risk with medical devices is that they can potentially expose both data and control of the device itself. This raises a tension between safety and security, which requires greater stakeholder collaboration to address, particularly in design and regulatory approaches. These stakeholders now include regulators, device manufacturers, healthcare organizations, IT suppliers, and patients themselves.

Risks are set to increase further with adoption of the Internet of Things (IoT) by healthcare organizations and consumers. The convergence of networking, computing technology and software has enabled increasing integration of Hospital Enterprise Systems/Information Technology (IT) and Clinical Engineering (CE), and suppliers through remote connectivity. This will be revolutionized by cloud based services and the use of 'big' data analytics.

The domain silos of IT and CE are being bridged by networking, exposing cybersecurity weakness and exacerbated by poor stakeholder communication, legacy technology, security vulnerabilities and inadequate device management. Medical device engineering has focused upon medical safety to safeguard patients, but has not sufficiently addressed cybersecurity, despite innovation. In fact, technology convergence is creating new attack pathways and cybersecurity risks with the implementation of new technology, yet older medical devices continue to be utilized, which are

Figure 1 – The changing landscape of healthcare cybersecurity



often not secure and are poorly managed. Increased connectivity, wireless technologies and 'hyper-connectivity' continues to create new opportunities for service delivery, remote monitoring and diagnostics, but may also create unforeseen consequences. Cyber incidents arising from potential adversaries, who may inflict cyber-attacks, have significantly increased.

Medical device security has become the primary healthcare security concern following a number of high profile incidents. Justifiably, given a device infected with malware has the potential to shut down hospital operations, expose sensitive patient information, compromise other connected devices and harm patients.

New approaches to dealing with increasing cybersecurity threats have recommended all parties collaborate to identify and assess cyber risks and threats, plan mitigations and appropriate incident response to ensure patient safety and security.

Changing scope of medical devices

Medical devices have changed from the once non-networked and isolated equipment, to devices with one-way vendor monitoring, to fully networked equipment with bi-directional communications, remote access, wireless connectivity and software. Indeed, the transition to software as a medical device (SaMD) has occurred[1].

EU and FDA definitions of devices exclude fitness, lifestyle and well being devices

When it's not a medical device

Both EU and FDA definitions of devices exclude fitness, lifestyle and wellbeing devices and applications. These may be considered as mHealth products: mobile health, utilizing connected mobile platforms such as mobile phones and tablets to run health applications. mHealth is considered a sub-segment of eHealth (electronic health), using information communications technology (ICT). Regulations have not kept pace with the rapid developments. Work is ongoing in Europe to determine a suitable legal framework. Meanwhile, the UK National Information Board Work Stream 1.2 road map is developing an assessment framework for digital applications[2]. The UK Medicines & Healthcare products Regulatory Agency provides comprehensive device determination guidance flow chart in the medical device stand-alone software including apps document.

Increasing cyber risk in healthcare

KPMG's 2015 cybersecurity survey reported 81% of healthcare organizations had been attacked in the past two years and only half felt adequately prepared[3]. The value of patient health information on the black market was the principal motivation. A recent dramatic increase in 'crypto ransomware', where criminals use malware to encrypt information and then demand payment via digital currency to recover information (including patient records) and restore operations, has affected hospitals in multiple countries, including the US, UK and Australia.

Unfortunately poor cybersecurity implementation could also affect patient health and inadvertently expose patient data. Technology convergence, embedding and mobile computing, coupled with the diversity of stakeholders have exacerbated the risk.

Medical device companies and healthcare organizations face an array of cyber threats including untargeted and increasingly sophisticated targeted attacks. Threats include:

- Disruption of care/service (including potential for patient deaths)
- Deception of staff with spoof email or fake websites to obtain login credentials or install malware
- Unintentional or intentional 'Insider threat', which can pose a significant threat due to the position of trust within an organization
- Loss of patient information – especially electronic protected health information (ePHI)
- Data breach, information exfiltration and loss of assets
- Blackmail, extortion and duress through exploitation of exfiltrated sensitive data
- Intellectual Property (IP) theft

Research has shown that healthcare cybersecurity continues to focus on the protection of patient health records, whilst failing to address the real threats to, or adequately protect patient health[4, 5]. A recent review by the UK National Data Guardian made recommendations concerning new data security standards featuring information security standards and frameworks[6]. The review did not address patient safety and medical devices.

Poor cybersecurity implementation could affect patient health

Staff may inadvertently introduce malware on to ill protected systems in untargeted attacks. Particularly where they are unpatched or unable to run anti-malware tools (in accordance with manufacturer instructions) and potentially use old software. However, adversaries will target the compromise of patient health records, whilst others may seek to compromise patient health or unintentionally impact it.

Who are the adversaries to healthcare and what are their motivations?

Threats come from a variety of different sources including; adversarial, natural (including system complexity, human error, accidents and equipment failures) and natural disasters[7]. Adversarial groups or individuals, also known as threat actors, have varying capabilities, motives, and resources:

- **Attackers** (includes those known as 'Hacktivists') – undertake attacks for thrill seeking, the challenge or to further an agenda. Tools have become more sophisticated, easier to use and freely available, leading to a dramatic increase in attacks from less technically knowledgeable individuals;
- **Bot-network operators** – take control of multiple systems to perform attacks and distribute phishing schemes, malware and spam. Services may be sold on for denial of service attacks or for relaying spam and phishing attacks;
- **Criminal groups** – organized criminals attack systems for monetary gain, these include spam, phishing schemes, spyware/malware attacks to commit identity theft and online fraud. Industrial espionage, ransomware and extortion with threatened cyber-attack are potential threats from criminals. Access as a service to networked systems could be sold on to third party criminals;
- **Foreign intelligence agencies** – use cyber tools for intelligence, espionage and to create various effects, including sabotage. Nation states have offensive capabilities supported by the intent to extend warfare to cyberspace. They may seek to utilize healthcare systems to obtain personal information and their activities may even harm patients;
- **Insiders** – employees and vendors who have unrestricted or less restricted access to systems and may be disgruntled or unintentionally introduce malware or undesirable changes;
- **Phishers** – individuals or groups that perform phishing schemes in order to steal identities and information for monetary gain;
- **Spammers** – send unsolicited email, possibly containing hidden or false information, conduct phishing schemes and denial of service attacks;
- **Spyware/malware authors** – produce and distribute malware for malicious purposes, often for monetary gain;
- **Terrorists** – seek to disrupt, destroy or exploit critical infrastructure to threaten national security. Terrorists may use spyware/malware and phishing schemes to fund activities;
- **Industrial spies** – seek to gain intellectual property and knowledge using clandestine methods. It is widely reported that some nation states and their proxies are very active.

Generic threats to the healthcare sector and specific threats to medical devices

Threats can be accidental or described as a result of non-validated changes. Such threats arise from insiders, outsiders and natural events. These are categorized as being passive or active. Passive would include information gathering or using tools to intercept or 'sniff' network data, such as passwords. Active threats come in many forms and include:

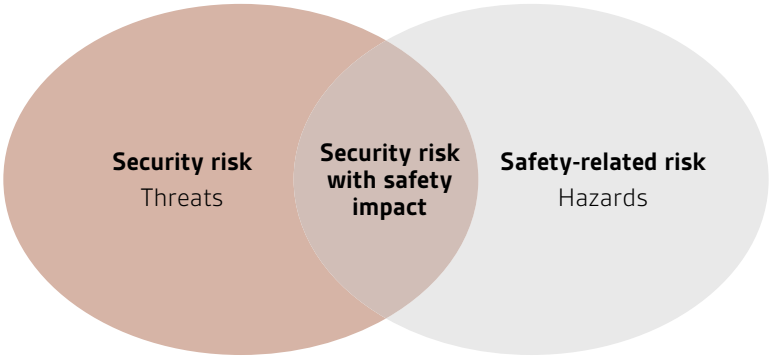
- **Communication** – disruption of network/device communications;
- **Database injection** – used to gain access to data or systems and to steal data;
- **Replay** – replaying data to gain access to systems or to falsify data;

- **Spoofing or impersonation** – a network term for fooling hardware or software making communication appear to originate from elsewhere;
- **Social engineering** – the attempt to obtain information by subterfuge from personnel that can then be used to attack computers, devices or networks;
- **Phishing** – a form of social engineering, using forged email or websites to entice the victim to reveal information;
- **Malicious code** – can have an number of purposes, to gather information, destroy data, provide a means to access a system, falsify system data or reports, or provide time-consuming irritation to operators and maintenance personnel;
- **Denial of Service (DoS)** – this affects the availability of networks and computing resources (e.g. operating systems, hard drives and applications);
- **Escalation of privileges** – a technique to increase the effectiveness of an attack by obtaining privileged access to perform actions that would otherwise be prevented;
- **Physical destruction** – attacks aimed at destroying or incapacitating physical devices or components. These might be direct or indirect via cyber-attack to cause actions that lead to physical damage (such as the Stuxnet malware).

Cyber security priorities for medical systems differ and relate to deployment. Confidentiality is a priority for hospital systems, preventing data breaches, or ransomware (which can also impact availability of systems if made unusable by encryption). Protection of the individual is a priority where patients are exposed to medical devices as part of their care, including implantable devices (Figure 2). Availability of such devices is a priority. 'Non-medical' or wellbeing devices, such as fitness trackers also have confidentiality as a priority, albeit with much lower impact.

Figure 2 – The relationship between security and safety risks

Adapted from *TIR57: Principles for medical device security – Risk management* © 2016 by the Association for the Advancement of Medical Instrumentation



Medical devices with embedded physical control functionality face unique threats that are similar to those identified for industrial control systems (ICS). Table 1 is based on threat events described in the US National Institute of Standards and Technology (NIST) Guide to Securing ICS[8].

Table 1 – Medical device example adversarial incidents – based upon NIST SP 800-82 Revision 2

Event	Description/risk
Malware on device/systems	Malicious software (e.g. Virus, Worm, Trojan, Ransomware) introduced onto the device or system
Denial of control action	Device operation disrupted by delaying or blocking the flow of information, denying device availability or networks used to control the device or system to healthcare staff
Device, application, configuration or software manipulation	Device, software or configuration settings modified producing unpredictable results
Spoofed device/system status information	False information sent to operators either to disguise unauthorized changes or to initiate inappropriate actions by medical staff
Device functionality manipulation	Unauthorized changes made to embedded software, programmable instructions in medical devices, alarm thresholds changed, or unauthorized commands issued to devices, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of devices and functions, or even disabling medical equipment
Safety functionality modified	Safety-related functionality manipulated such that they do not operate when needed; or perform incorrect control actions, potentially leading to patient harm or damage to medical equipment

Medical device security incidents

Security configuration error causes device failure

A report by the U.S. Food and Drug Administration (FDA) which is responsible for medical device oversight highlights the life threatening danger of security failures[9]. A diagnostic computer used to monitor, measure and record physiological patient data failed whilst being used for cardiac catheterization procedure. There was a delay in the procedure whilst the application was rebooted. The investigation found that communications between the patient device and the monitor were lost for five minutes while the patient was sedated, with no physiological data presented. The delay in care could potentially harm a patient. However, the procedure was successfully completed on rebooting of the application. A configuration error of the anti-virus scan included directories that caused deletion of critical patient data. The manufacturer reported the cause to be the customer not following anti-virus software installation instructions.

Potential exploitation of cybersecurity vulnerabilities could affect how a medical device operates

Security vulnerabilities identified in implantable cardiac devices and wireless transmitter

The FDA has provided recommendations concerning the potential exploitable vulnerabilities in radio frequency (RF) enabled St. Jude Medical implantable cardiac devices and the corresponding Merlin@home Transmitter. The St. Jude Medical Merlin@home Transmitter connects wirelessly to the patient's implanted cardiac device to read data, which is then sent via the home network to the medical facility via the Merlin.net Patient Care Network using either landline, mobile, or wireless ('wi-fi') internet connections. In common with other medical devices, embedded computing is increasingly vulnerable to cybersecurity intrusions and exploits, facilitated by pervasive internet connectivity. Potential exploitation of cybersecurity vulnerabilities could affect how a medical device operates.

The FDA review of the St. Jude Medical's Merlin@home Transmitter confirmed should the vulnerabilities be exploited, an unauthorized user could remotely access a patient's RF-enabled implanted cardiac device by altering the Merlin@home Transmitter. The altered Merlin@home Transmitter could then be used to modify programming commands sent to the implanted device, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks. A validated software patch has been issued that will automatically update the Transmitter. The report states there have been no reports of patient harm resulting from these vulnerabilities[10].

Ransomware attack created patient safety issue

The US based MedStar Health provider received bitcoin demands following encryption of computer systems. Notifications were displayed on infected computers, threatening loss of data after 10 days. Patient records for 10 hospitals and 250 outpatient centres were reported to be either unavailable and or could not updated, whilst MedStar used backups to restore data. Patient operations were cancelled and ambulances diverted. Nurses and doctors highlighted safety issues concerning delays to test results affecting treatment[11].

Security vulnerabilities enable network attacks and potentially fatally alter drug dosing

Announcements made by the US Department of Homeland Security concerning security vulnerabilities of a Hospira hospital drug pump, discovered by a security researcher, raised concerns about other medical devices including insulin pumps and pace makers[12]. Following a low-risk wireless vulnerability disclosure, Johnson and Johnson contacted customers to mitigate the potential threat of remote dosing from their Animas OneTouch Ping insulin pump system[13]. Reports have also highlighted the extraction of patient data from medical devices and their use as conduits to attack hospital networks[4]. The significance of these announcements regarding the medical device vulnerabilities is the potential to alter drug dosing with lethal consequences.

Medical device cybersecurity risk management

The FDA Postmarket Guidance recommends manufacturers implement a process for assessing cybersecurity risk to the device's essential clinical performance by considering[14]:

1. the exploitability of the cybersecurity vulnerability; and
2. the severity of the health impact to patients if the vulnerability were to be exploited.

However, estimating the probability of a cybersecurity exploit is problematic in the absence of data on the probability of the occurrence of harm. This difficulty applies to software failure and situations, such as sabotage or tampering with a medical device, as highlighted in BS EN ISO 14971: 2012 *Medical Devices – Application of Risk Management to Medical Devices, Annex D*[15]. The approach in BS EN ISO 14971 is to use the worst possible case outcome or the default value for the probability as one. According to UK CPNI guidance (to be replaced by National Cyber Security Centre (NCSC) security principles), worst-case scenarios drive the cyber-protection level of the device. Therefore, all malicious attack scenarios are gathered and compared to human-error 'misconfiguration' scenarios. The security control measures should cover the worst parts of that collection.

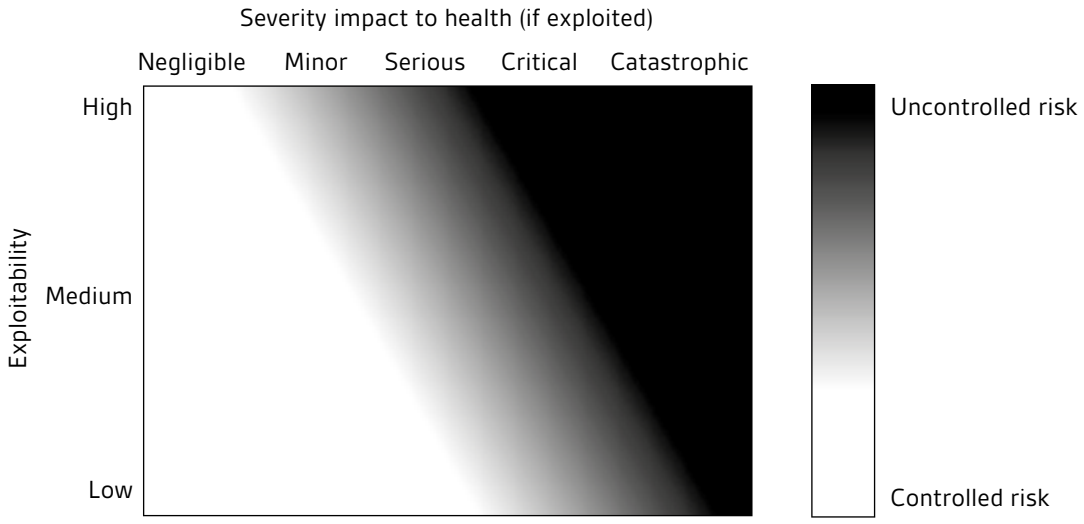
The FDA recommends manufacturers should consider using a cybersecurity vulnerability assessment tool or similar methodology for rating vulnerabilities and determining the need and urgency of a response. The Common Vulnerability Scoring System, Version 3.0 is specifically identified, amongst others, and provides numerical ratings (equivalent for high, medium and low) that incorporate factors used in assessing the exploitability[16]. For assessing the severity impact to health, the FDA suggests the approach based on qualitative severity levels as described in BS EN ISO 14971 (and further extended in IEC 8001 2-2) and offers the following descriptions (Table 2)[14]:

Table 2 – Qualitative severity levels – U.S. Food and Drug Administration Postmarket Management of Cybersecurity in Medical Devices Guidance

Common Term	Possible Description
Negligible	Inconvenience or temporary discomfort
Minor	Results in temporary injury or impairment not requiring professional medical intervention
Serious	Results in injury or impairment requiring professional medical intervention
Critical	Results in permanent impairment or life-threatening injury
Catastrophic	Results in patient death

The vulnerability risk assessment is used to evaluate the whether the risk to essential clinical performance of the device is controlled (acceptable) or uncontrolled (unacceptable). In Figure 3, the exploitability and severity impact to health represents risks that are controlled or uncontrolled. Manufacturers are recommended to make a binary determination on whether a particular vulnerability is either controlled or uncontrolled using an established process that is tailored to the product, its essential clinical performance and the situation. Risk mitigations, including compensating controls, should then be implemented as necessary to reduce the residual risk to an acceptable level. In certain cases the manufacturer should report the cybersecurity vulnerabilities.

Figure 3 – Evaluation of Risk to Essential Clinical Performance – U.S. Food and Drug Administration Postmarket Management of Cybersecurity in Medical Devices Guidance



Tensions in safety and security convergence

A generic safety assessment considers the likelihood that a hazardous event will occur (frequency or duration) and the severity of the resulting incident or harm. Safety-related devices or systems are generally concerned with non-malicious faults, and how these can be avoided or mitigated. Safety-related systems and applications implement safety functions that act on the process under control to prevent identified hazardous events from occurring. The calculated probability that an undetected fault will lead to the loss of a safety function, when required is probabilistic, quantitative and seldom changes.

Conversely, security addresses the intelligent malicious attacks to a system by identifying the adversaries (otherwise known as threat actors), their capabilities, intent and resources, compromise methods and the vulnerabilities that may be exploited. This considers the likelihood that a threat will exploit a vulnerability leading to a (business) impact/consequence. The result is qualitative and changes dynamically as potential adversaries, intent or capability change and as vulnerabilities are discovered and exploits are developed.

Several challenges arise in convergence and implementation. Not least, the separation of the safety and security engineering disciplines. However, tension is illustrated in the static and probabilistic nature of safety engineering versus the dynamic qualitative security assessment and treatment. There are implications for the management of safety certification and security of devices or systems in operation and therefore the need to proactively manage security incidents. Also, the approach of an intelligent adversary could consider the range of highly improbable events and use those as goal based outcomes. Thus, undermining safety protection measures or intentionally triggering known safety functions (e.g. fail safe or safe motion) to create apparent failures and potentially denying use.

Safety-related denial of service has already been illustrated by researchers investigating the cybersecurity of teleoperated robotic surgery[17]. Eavesdropping and subsequent hijacking of communications (Man in The Middle attack) between the remote surgeon and robot successfully taking control and triggering an emergency-stop through fast (unsafe motion) movement or motion beyond zoned safety areas. These actions caused the robot to shut down in a fail-safe mode, in the same manner as an industrial robot[18]. This would force a reset of the safety system to commence further surgery. By sending a malicious packet, the researchers were able to prevent the robot from being reset, preventing additional surgery from being performed. Automated medical devices are in fact control devices (Operational Technology), which have the highest possible impact as consequence of failure. Industrial control systems/SCADA/Operational Technology guidance is particularly relevant.

The AMMI has recently published specific medical devices guidance that mirrors the more detailed approach in development for control systems, to bridge safety and security risk management[19] (Figure 6).

Can medical devices be insecure and safe?

Corporate business systems (IT) are often assessed primarily for the security risks to the confidentiality of information they process, for example, the protection of contractual information, patient data, intellectual property or personnel records. The consideration of risks to integrity of information, that it is correct and untampered with, and availability (accessibility of the information) may not be foremost. Whereas, medical devices and embedded systems with physical functionality, the priority is safe operation, the avoidance of injury or death, system or device availability (such as class 3 devices such as pacemakers), device or machine protection, operation/production and time-critical responsiveness in real-time operation[20].

The traditional information assurance approach of Confidentiality–Integrity–Availability (CIA) with respect to the corporate environment does not emphasize these factors. For Cyber Physical Systems (CPS), such as medical devices, it is also necessary to consider the Safety, Reliability and Availability (SRA) of the processes, devices and connected systems. It must also include any safety functions and assess the consequences of malfunction to people, equipment and environment, cognisant of the legal onus upon the manufacturers, integrators, IT suppliers and healthcare organizations throughout the systems lifecycle[21].

These different domain views highlight an important distinction: when the IT security team considers risk, such as availability, they are generally referring to the information from an Information Security or IT Security perspective

Controlling access to systems and information or data is key

(information risk). Whilst for clinical engineering and medical device functionality, availability will be referring to the medical systems/devices or processes and potentially the safety functions used to prevent hazardous operation and control risks leading to physical harm. The same words are used but not with the same meaning. There is a need to collaborate and share a common lexicon and understanding. The controls or countermeasures employed for security mitigation would need to be assessed for their impact, particularly on safety functionality, in order that new hazards are not introduced. This may require the re-design of the safety functions to address the security induced hazards, and is a specific requirement of the mother of functional safety standards, IEC 61508[22]. The technical specification IEC TS 63069 is developing a framework for bridging safety and security and is expected to have board applicability.

It may be that security risk assessments should no longer focus on the information as the primary asset to be defended, but explicitly consider the health care outcomes, systems and processes for which that information is used. A balance needs to be achieved with safety and security, and privacy. In many risk assessments, this is achieved indirectly by assessing the business impact/consequence, however, information security frameworks do not explicitly address safety risks. The security approach to medical devices needs to also address the cyber physical aspects, not only (patient health) information.

An alternative assurance model that combines engineering good practice with information security is the modified Parkerian Hexad for cyber physical systems (operational technology), which added the Safety and Resilience attributes, noting Availability includes reliability[22]. The resulting assurance model is shown in Figure 4, where the eight facets address safety and security from three perspectives.*

The eight facets are:

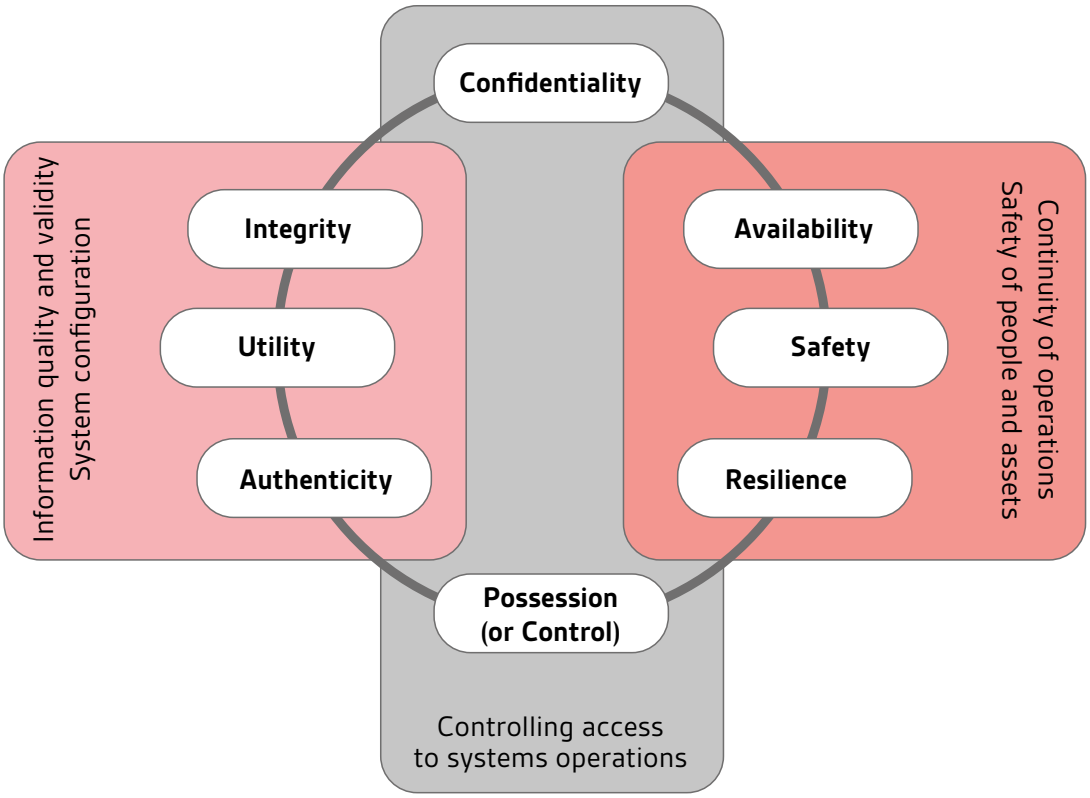
- **Confidentiality** – the control of access to and prevention of unauthorized access to systems and information or data;
- **Integrity** – maintaining the consistency, coherence and configuration of information and systems, and preventing unauthorized changes to them;
- **Authenticity** – ensuring that inputs to and outputs from systems, the state of the system and any associated processes, information or data are genuine and have not been tampered with or modified;
- **Utility** – ensuring that the system and any information or data remain usable and useful across the lifecycle of the system and where appropriate can be transferred to any successor system(s);

*The modified Parkerian Hexad extends the cybersecurity objectives for cyber physical systems (operational technology) beyond the traditional information assurance CIA triad, to include safety and resilience attributes.

- **Availability** – ensuring that the systems, information or data, and associated processes are consistently accessible and usable in an appropriate and timely fashion. To achieve the required availability may require each to have an appropriate and proportionate level of resilience;
- **Possession (or Control)** – the design, implementation, operation and maintenance of systems and associated processes so as to prevent unauthorized control, manipulation or interference;
- **Resilience** – the ability of the systems and information or data to transform, renew and recover in timely response to adverse events; and
- **Safety** – the design, implementation, operation and maintenance of systems and related processes so as to prevent the creation of harmful states which may lead to injury or loss of life, or unintentional environmental damage.

Figure 4 – Cyber physical assurance framework based on the Parkerian Hexad*

Courtesy of Hugh Boyes – Cybersecurity and Cyber-Resilient Supply Chains. Technology Innovation Management Review, 2015



Healthcare technology challenges

In the event of older isolated non-networked devices running proprietary systems and software, cybersecurity risk was considered low and safety risk was paramount, as medical device regulations demonstrate. Technology convergence has since brought an abundance of commercially off-the-shelf (COTS) technology including common networking infrastructure, operating systems, software, smart mobile devices, computers and embedded control systems to medical devices. Many medical devices contain configurable embedded computers that might be vulnerable to cybersecurity breaches. Often embedded systems may utilize older, vulnerable operating systems that may be unpatched or even no longer supported. There is now increased risk due to connectivity of medical devices to the internet, hospital networks, other medical devices, mobile computing and phones. This according to the FDA may lead to the following that could affect medical devices and hospital networks:

*The modified Parkerian Hexad extends the cybersecurity objectives for cyber physical systems (operational technology) beyond the traditional information assurance CIA triad, to include safety and resilience attributes.

- network-connected/configured medical devices infected or disabled by malware;
- the presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices);
- security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection.

Furthermore, FDA post market guidance introduces the concept of essential clinical performance, linking safety and cybersecurity:

> *'Essential performance means performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk. Compromise of the essential performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm.'*[14]

Regulation

US Food and Drug Administration

The FDA has issued several sets of guidance, demonstrating that medical device cybersecurity is a significant issue. Both the post-market management of cybersecurity in medical devices and the interoperable medical devices contain specific guidance on cybersecurity. The FDA recommends manufacturers use the NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity, which builds on earlier guidance for Industrial Control Systems.

In the *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, the FDA stated effective cybersecurity is important to assure medical device functionality and safety with the increasing use of wireless, internet and network connected devices, along with the frequent electronic exchange of medical device-related health information. The guidance is intended to assist industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices. Manufacturers are recommended to establish a cybersecurity management approach for risk analysis, vulnerability assessment, mitigation, design and validation.

Both the pre-market guidance (October 2014) and the post-market guidance (December 2016), recommend manufacturers utilize the NIST Framework for Improving Critical Infrastructure Cybersecurity. This has core functions to guide an organization's cybersecurity activities: Identify, Protect, Detect, Respond and Recover. The new NIST Cybersecurity Framework (CSF) (draft revision 1.1) places greater emphasis on managing supply chain risk.

The NIST CSF maps reference standards for specific elements and various other frameworks including the Health Insurance Portability and Accountability Act (HIPAA) 1996 (US legislation that provides data privacy and security provisions for safeguarding medical information). The intent is to promote collaboration amongst the medical device and health IT communities and develop a common understanding of cybersecurity vulnerabilities and risk. This will improve assessment of patient safety and public health risks and ability to take timely and appropriate mitigation actions.

European Union Regulation

EU regulation lags behind the US FDA recommendations. However, the Medical Devices Regulations (MDR) to be published in 2017 significantly enlarges the scope of applicable devices, and will define more stringent post-market

surveillance, as will the draft Regulation on in vitro diagnostic medical devices. The draft plans have provisions for vigilance, market surveillance and reporting in respect of serious incidents and implementing safety corrective actions. Member states will be required to analyse and risk assess incidents, the adequacy of corrective actions, and any further corrective action that may be required. Member states will also monitor the manufacturer's incident investigation. General safety and performance requirements prohibit the compromise of patient safety and include the application safety principles; taking account of state of the art and identifying known or foreseeable hazards and risks from intended and foreseeable misuse. Any remaining risks are to be reduced as far as possible by taking adequate protection measures.

The regulations do specifically stipulate devices incorporating software and the requirement to implement 'state of the art' (albeit at a high level, referring to information) security, protection against unauthorized access and ensure intended operation. The regulations also highlight risks from external influence (including electrical and radio) and negative interaction of software and its operating environment. As such the draft regulations seek to address the consequences of cyber incidents and the foreseeable safety hazards. Confidentiality of personal data is to be undertaken in accordance with the EU Data Protection Directive for both implementations. Member States will implement 'effective, proportionate, and dissuasive' penalties for infringement.

The current EU Medical Devices Directive does not explicitly reference cybersecurity, focusing upon safety risk assessment. The European-harmonized ISO standard BS EN ISO 62304 *Medical device software — Software life-cycle processes* includes security provisions. The European standard for the application of risk management to medical devices BS EN ISO 14971:2012 highlights that probabilities are very difficult to estimate for software failure, sabotage or tampering.

Medical device incidence reporting to regulators focuses on safety, not security. Obtaining suitable data to support estimations is therefore highly likely to be problematic. The international standard used by regulators for medical device surveillance in the post-market phase (DD ISO/TS 19218-1:2011+A1:2013) for sharing and reporting adverse incidents by users or manufacturers, does not offer cyber specific categorization. Arguably, a cyber incident could be identified with any of the following categories: computer hardware, computer software, electrical/electronic, external conditions, incompatibility issues, non-mechanical, loss of communications, incorrect device display function, installation, configuration, performance deviation, output issue, protective alarm or fail-safe issue, unintended function – resulting in malfunction, misdiagnosis or mistreatment, or simply as 'other device issue'.

Medical device incidence reporting focuses on safety, not security

This of course assumes that the incident in question is fully understood. It is certainly possible that a medical device could appear to operate normally during and after cyber tampering. It may just seem faulty to a clinical technician, who is probably anticipating a fault condition, rather than malware or a cyber-intrusion.

The new EU Cybersecurity Directive (Directive on security of network and information systems) came into force in August 2016, giving Member States 21 months to implement it into national law. A further six months is provided to identify 'operators of essential services'. Market operators identified in the health sector will be need to comply with mandatory security breach and incident notification requirements to competent authorities, i.e. regulators, and will be required to implement appropriate organizational risk management, technical and security measures. The Directive duplicates some of the provisions in the EU General Data Protection Regulation (GDPR) on personal and sensitive information and the requirement to notify regulators of security breaches (due 2018). The Cybersecurity Directive is likely to be considered the minimum cybersecurity standard by most organizations operating in the EU[23].

Managing medical device cybersecurity

Medical device manufacturers and healthcare organizations need to implement safeguards to reduce the risk of failure or misuse in the event of a cyber-attack. The FDA has issued recommendations referencing the NIST Industrial Control Systems Security Guide published in June 2015. In the UK the Centre for the Protection of the National Infrastructure (CPNI) also updated applicable guidance in 2015: Security of Industrial Control Systems. Responsibility for cybersecurity has now transitioned to the UK's new National Cybersecurity Centre (NCSC), which incorporates the former CESG, CPNI (cybersecurity function) and UK CERT. The NCSC provides a framework of good practice guidance, including generic guidance such as the 10 Steps to Cybersecurity. In the UK, NHS Digital provides security guidance focused presently on IT networks and clinical risk management[24, 25].

Why is Industrial Control Systems guidance being recommended? There are many similarities, which include the requirement to protect embedded computers used to monitor and control physical systems. Control system security goals focus on control system availability, equipment protection, operations (even in a degraded mode) and time-critical system response. The measures used to implement safeguards are equally applicable and are focused towards an operational technology environment (in this case medical devices and health networks) as opposed to traditional IT Information Assurance. IEC 62443-3-3 security controls are combined with others in IEC/TR 80001-2-8 for the risk management of IT networks, which incorporate medical devices. The potential security impacts of security measures are outlined to distinguish control systems, in that their application should not cause the loss of essential services and functions, including emergency procedures.

IEC 62443-1 describes the basic concepts and models related to cybersecurity that are used throughout the IEC 62443 series. A key concept in IEC TS 62443-1-1 is the application of security zones and conduits used to describe the various operational components and how they are connected. The zones are logically group assets within the enterprise, which can then be analysed for security policies and requirements. The architecture model provides context for assessing common threats, vulnerabilities, and the corresponding countermeasures needed to attain the level of security required to protect the grouped assets.

The audience for these standards includes asset owners, system integrators, product suppliers, service providers and compliance authorities. Recommendations include network segmentation (applicable to IT networks versus clinical networks and enclaves), but also covers secure design, implementation of security, including governance, risk assessment, procurement, managing the system lifecycle, maintenance, third party risk and incident management.

Procurement

Healthcare organizations and medical device manufacturers can benefit from working towards a common set of security expectations. This can be facilitated by the use of a common procurement language and guidelines to ensure security is integrated into medical devices and systems.

The US Department of Homeland Security (DHS) developed the cybersecurity procurement language for control systems. The document provides an introduction to control systems and outlines escalating risk to control systems

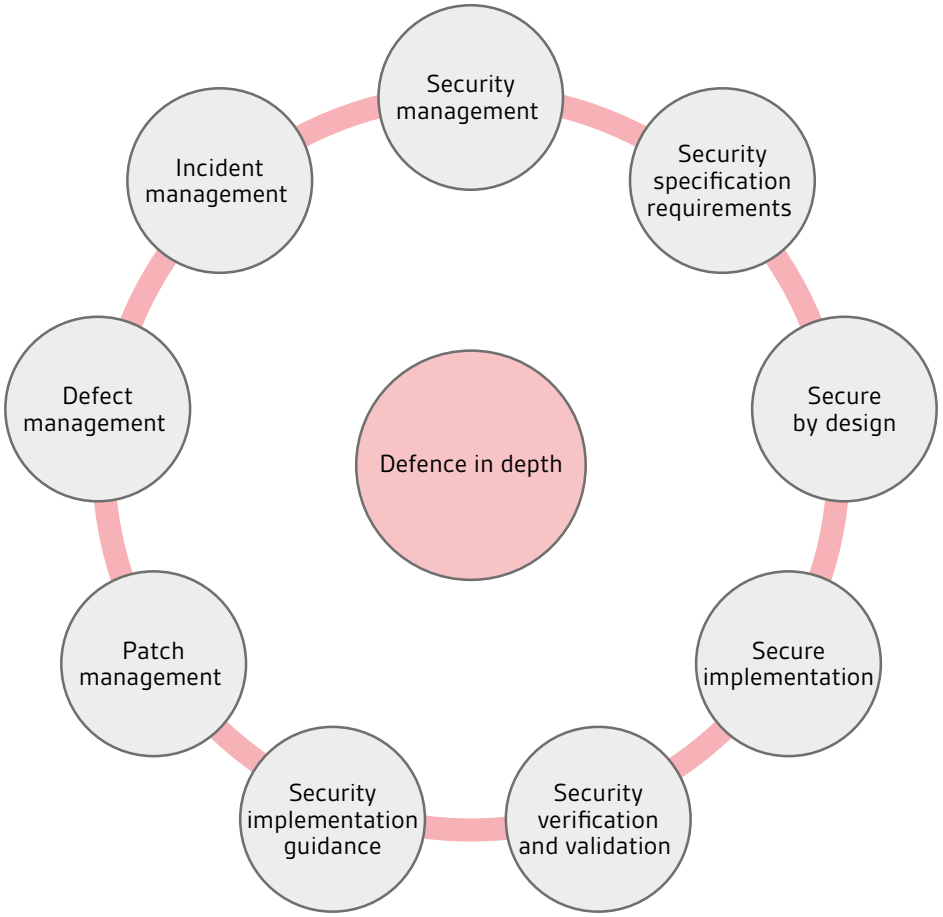
and security objectives with a control systems perspective. A similar approach for medical devices could provide specification language for use in procurement specifications, covering all aspects of cybersecurity, including acceptance testing, verification, integration, maintenance guidance and any supporting references (guidelines, regulation or standards)[26].

Healthcare organizations have the opportunity to stipulate baseline practices and for vendors to demonstrate adoption of secure development processes, device or system hardening and lifecycle management. Cybersecurity standards developed for industrial control systems vendors and their products (IEC 62443-4-1 and IEC 62443-4-2) can be used to set expectations for supplier secure product development processes and embedded device security assurance.

Secure product design and lifecycle management

Medical devices manufacturers can apply a variety of secure product development lifecycles (SDLC) good practices. Cybersecurity assurance programmes can utilize the good practice developed in IEC 62443-4-1 Product Development Requirements and IEC 62443-4-2 Technical Security Requirements for industrial control system components. These standards focus upon secure product development good practice, (including IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems), verification and testing, and lifecycle management (Figure 5).

Figure 5 – Defence in depth philosophy for secure product lifecycle



The IEC 62443 approach defines a secure development lifecycle (SDL) including security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. Importantly, these requirements are applicable to the product developer and maintainer, but not to the user of the product. The standard also defines a capability maturity assessment to benchmark suppliers.

NIST recently published *Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (SP 800-160). It provides an engineering perspective and describes the actions necessary to develop more defensible and survivable systems, in light of the growing adverse consequences of cyber-attacks, disruptions and hazards, where the need for trustworthy secure systems is paramount.

Security topics are addressed in the context of the system life cycle processes contained in ISO/IEC/IEEE 15288 and the security-related activities and tasks that are described in SP 800-160, which is designed as complementary guidance. It is intended to be flexible in application acting as a handbook for achieving identified security outcomes in an engineering perspective on system lifecycle processes. Further publications in the SP 800-160 series are planned to cover other security engineering topics in the lifecycle context of ISO/IEC/IEEE 15288.

Notified Bodies

Notified bodies are increasingly addressing security in embedded devices. Basic safety standards for functional safety, utilized across other industrial sectors, are now addressing cybersecurity throughout system lifecycles and recommend approaches to secure products, systems and networks. They also reference IEC 62443 (cybersecurity for control systems) for cybersecurity implementation and control measures. Assessments of medical devices need to incorporate both safety and security risk assessments and mitigation. IEC 62443-1-3 currently under development will bridge safety and security requirements. The working group is liaising with other application sectors in order that it can be widely applicable.

Security assessments should also consider an organization's cybersecurity maturity, and approach to cybersecurity in products, and extend the Quality Management Systems audit, as per the Medical Device Single Audit Program (MDSAP) Pilot[27]. This will highlight areas of capability and those requiring development, which can then be prioritized. The Cybersecurity Capability Maturity Model (C2M2) is one such assessment tool, which can be used to support the NIST Cybersecurity Framework implementation. Developed by the US Department of Energy in cooperation with Department of Homeland Security, it is transferrable to other domains to enhance cybersecurity, and is freely available. It assists in prioritising activity and investments to improve cybersecurity. C2M2 can be used to assess cybersecurity programme sophistication, culture and institutionalization; including programme management and organizational governance[28].

In turn, the implementation of security practices in the development and implementation of medical devices can also be evaluated using a relevant cyber maturity framework that is focused upon building security into products and used to measure security activities against those most commonly performed using mature software security initiatives. Building Security in Maturity Model (BSIMM) is such a software security framework which considers four domains: Governance, Intelligence, SDL Touchpoints and Deployment[29]. Cyber maturity frameworks can also be used to assess vendors. The BSIMM framework includes an approach specifically designed for vendor management of third party software, extending beyond the shortcomings of penetration testing as a security measure.

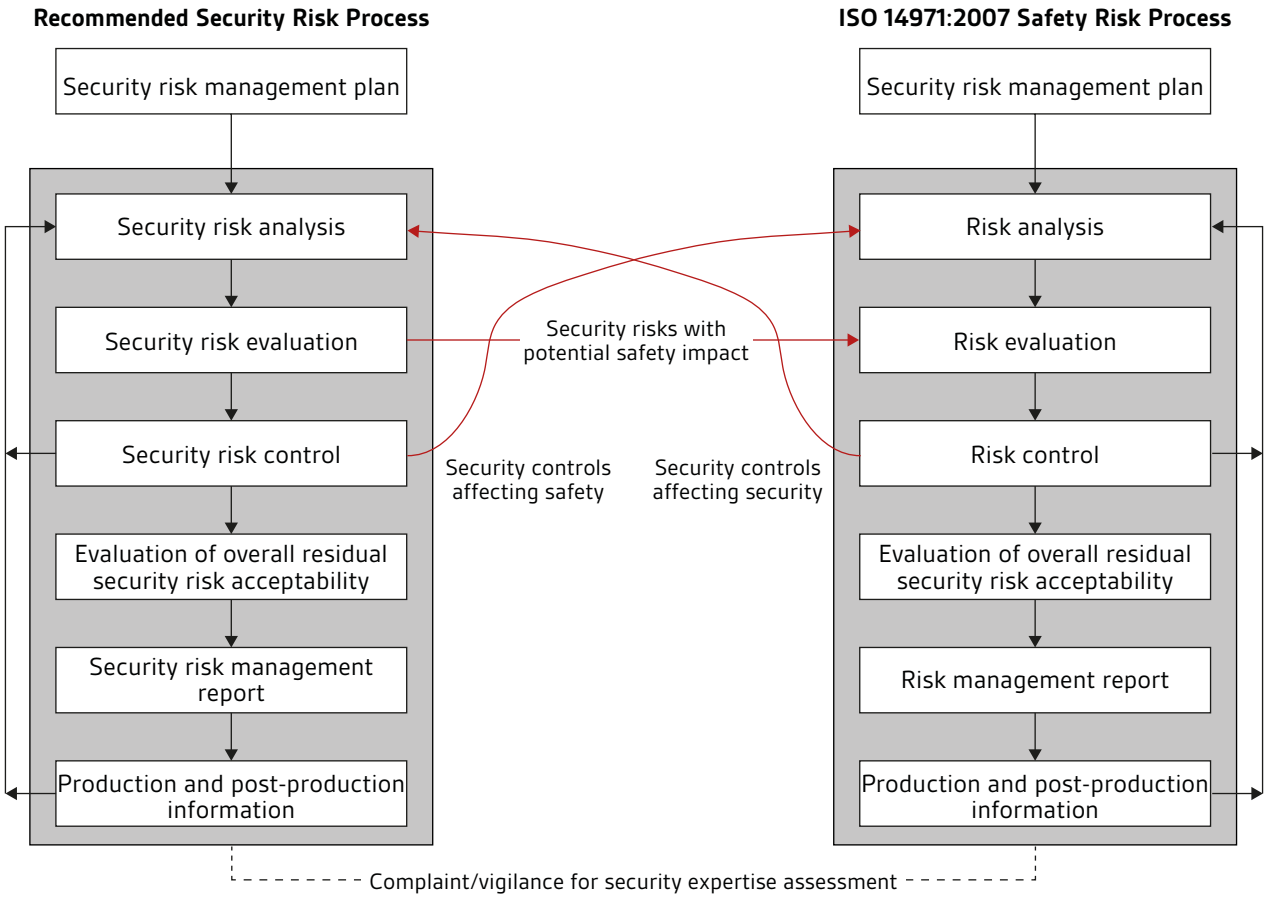
Device manufacturers/vendors

The predicted rapid growth of connected devices in healthcare applications, the increasing concern over breaches of patient data and more recently the potential risks to patient safety requires security to be critical feature of medical products and software. Healthcare procurement will be more sophisticated in their demands and will also desire for appropriate responses to security incidents. Anticipate the development of the 'intelligent customer'* as a management function that fully understands cybersecurity requirements, having specified the requirements, supervised the procurement and integration and has the ability to technically review all facets of the security

*The concept of intelligent customer (IC) was developed by UK Office for Nuclear Regulation and the UK Health and Safety Executive. The concept is used by the UK Government for IT procurement and has gained international acceptance. http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-049.pdf

Figure 6 – Managing safety and security risk convergence

From *TIR57: Principles for medical device security – Risk management* © 2016 by the Association for the Advancement of Medical Instrumentation



lifecycle. Healthcare procurement will increasingly focus upon security, given high profile incidents, and the launch of assurance services, which seek to offer third party validation and verification.

Manufacturers and suppliers should view cybersecurity as a business enabler and potentially as an opportunity to differentiate in the medium term. The poor handling of security incidents can rapidly become public knowledge and damaging to corporate reputation, with predictable downsides. Therefore, developing incident response strategies, processes and support mechanisms to deal with inevitable security issues is an absolute requirement. This has already occurred in the industrial control systems sector, where the market was quick to assess vendor responses to cybersecurity incidents after Stuxnet, the malware that targeted Iranian centrifuges[30].

Information sharing

Data sharing is essential for high quality healthcare and care services. Mandatory reporting is already a requirement for some, as noted earlier. However, collaborative sharing between all stakeholders is recommended to facilitate early mitigation. Timely sharing of information can provide actionable threat intelligence, enhancing situational awareness and permit pre-emptive activities to address cybersecurity vulnerabilities.

In the UK CareCERT has been analysing threat intelligence and broadcasting advisories to health and care organizations since late 2015. It also provides national cybersecurity incident management. In September 2016,

CareCERT launched Assure, React and Knowledge services to support implementation of the new Data Security Standards for Health. These added risk assessment, mitigation and incident response advice, along with cybersecurity eLearning services. Early adopters are encouraged to register.

Organizations and individuals can also participate in information sharing. In the UK, the NCSC operate the Cyber-security Information Sharing Partnership (CiSP), formerly it was a CERT UK function. It is a joint industry and government initiative to exchange cyber threat information in real time, in a secure and confidential environment. The US National Health Information Sharing and Analysis Center (NH-ISAC) operates in collaboration with the FDA, and is a non-profit organization that provides members with actionable information on cybersecurity and coordinates cybersecurity incidence response. The organization also provides cybersecurity tools, guidance via members, events and access to special interest groups.

Conclusions and recommendations

Much of the medical devices guidance is recent and still in development. There is convergence, not only from a technology perspective, but amongst healthcare stakeholders and the recognition that cybersecurity is a collaborative journey. Where addressing medical device risk has formerly focused on functional safety, and safety-related risk (to the exclusion of cybersecurity) or the protection of data, multiple approaches are now actively addressing the lifecycle risks and potential harm from cybersecurity incidents. Medical devices manufacturers are recommended to undertake a cybersecurity maturity assessment to identify and prioritize areas for improvement. This should include product lifecycle security, stipulated in emerging assessment schemes, which will be articulated in healthcare procurement. Mature incident response plans and processes are essential for all healthcare entities, in anticipation of the inevitable cybersecurity event.

Resources

Cybersecurity lexicon for converged systems

CIA Information security policy objectives: Confidentiality, Integrity and Availability

Computer virus A program that is run (unwittingly) by the user that executes on the victim system and spreads to other executable programs.

Crypto ransomware Criminals use malware to encrypt information and then demand payment via digital currency to recover information.

Cyber physical systems (CPS) CPS interface the physical world with the logical, enabling the (Industrial) Internet of Things, data and services. See Operational Technology.

Backdoor Provides access to a compromised system normally via the internet bypassing legitimate authentication (logon).

Botnet A large number of compromised systems attack a single target. The Mirai botnet attack used IoT devices, mainly home routers and cameras to create a DDoS.

Denial of Service (DoS) An incident where there is an interruption in services or access to a resource, normally with malicious intent. In a distributed denial of service (DDoS) attack, large numbers of compromised systems (called a botnet) attack a single target.

ePHI Electronic protected health information (ePHI) refers to protected health information (PHI) from the US Health Insurance Portability and Accountability Act 1996

Exploit kit An exploit kit automates the exploitation of browsers and software 'plug-ins' used with them. They are often user-friendly and can be used by non-technical people to run a crime campaign, which might include using compromised machines as a remote platform to launch further attacks.

Functional safety The freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly. Functional safety is the part of the overall safety that depends on a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes.

Hacktivist Short form of *hack*er ac*tivist* – an individual or group that uses computer networks to further their political agenda.

Internet of Things (IOT or IoT) The movement toward connecting physical devices – including the car, fridge, home heating system, lighting, fitness, wellbeing and medical devices etc. – to the internet so that they can be controlled, monitored or supported remotely.

Industrial Internet of Things (IIOT or IIoT) The use of the Internet of Things (IoT) in an industrial capacity. Industrial IoT systems are bound by specific design functionality, and can therefore be distinguished from (non-Industrial) IoT ad hoc groupings of existing devices sharing data to fill an emergent requirement.

Industrial control systems (ICS) Also known as Operational Technology or OT. The systems that control industrial and critical infrastructure. A generic term that encompasses several types of control systems used in industrial sectors and critical infrastructure.

Keyboard/Mouse Jack The compromise of a wireless keyboard or mouse, where an attacker can circumvent poor or lack of encryption to inject or read key strokes.

Keylogger Software or hardware that records keystrokes made by a computer user, which can be used to obtain passwords and other confidential information.

Malware Short for *mal*icious soft*ware* – refers to any intrusive or hostile software.

Man in The Middle attack (MiTM) An attacker intercepts and relays messages between two parties who believe they are communicating directly with each other.

Medjack The compromise of vulnerable medical devices for use as back doors; providing malicious access to hospital networks.

Operational Technology (OT) IT derived term to distinguish embedded control systems from information processing systems. Comprises the hardware and software that controls or monitors the state of a physical system. See industrial control systems.

Penetration testing The testing of computer devices, systems, networks or web pages to assess potential vulnerabilities that could be exploited to provide access.

Phishing Spam email either containing malicious software or links to websites with malicious software.

Remote access trojan (RAT) A trojan can provide access to a target computer, in order to download additional malicious software, which may (amongst other things) encrypt files (ransomware), monitor computer use and control the computer remotely, potentially for attacks on other computers.

Rootkit A software package that conceals the presence of malicious software on a computer.

Social engineering The attempt to obtain information by subterfuge from personnel that can then be used to attack computers, devices or networks.

Spear-phishing Carefully crafted email sent to selected individuals either containing malicious software or links to websites with malicious software.

Spoofing or impersonation A network term for fooling hardware or software, making communication appear to originate from elsewhere.

SRA Traditional engineering objectives: Safety, Reliability and Availability.

Trojan A trojan horse or trojan is any malicious program that is concealed and run by the user.

Update hijack Legitimate software updates compromised with malicious software.

Waterhole attack An attack targeted at a particular group of individuals, who visit common websites. A chosen website is compromised in anticipation that it will be visited by a member of the target organization.

Worm A malware program that spreads itself (without user intervention).

Agency guidance and security advisories

- European Union Agency for Network and Information Security (ENISA) www.enisa.europa.eu
- UK CareCERT http://content.digital.nhs.uk/carecert
- UK Cyber-security Information Sharing Partnership https://www.ncsc.gov.uk/cisp
- UK Medicines and Healthcare products Regulatory Agency https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency
- UK National Cyber Security Centre https://www.ncsc.gov.uk/guidance
- UK NHS Digital http://digital.nhs.uk/
- US DHS ICS-CERT https://ics-cert.us-cert.gov/
- US FDA Cybersecurity guidance http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
- US National Health Information Sharing Analysis Centre https://nhisac.org/

Recommended guidance

- AAMI TIR57:2016 Principles for medical device security – Risk management
- IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models
- IEC 62443-2-1:2010 Industrial communication networks - Network and system security – Part 2-1: Establishing an industrial automation and control system security program

- IEC TS 63069 Industrial-process measurement, control and automation – Framework to bridge the requirements for safety and security – Forthcoming
- PAS 555:2013 Cybersecurity risk. Governance and management. Specification
- NCSC Security Architecture Principles for OT, March 2017
- NCSC Password Guidance: Simplifying Your Approach, September 2016
- NIST (National Institute of Standards and Technology) Cybersecurity Framework (the Framework), February 2014 & Draft version 1.1, January 2017
- NIST SP 800-53 Rev 4 Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
- NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security, May 2015
- NIST SP 800-160 Systems Security Engineering, November 2016
- NIST SP 800-183 Network of 'Things', July 2016, July 2016
- US DHS ICS-CERT https://ics-cert.us-cert.gov/Standards-and-References

Applicable standards, technical specifications and reports

- PAS 277:2015, *Health and wellness apps – Quality criteria across the life cycle – Code of practice*
- EN ISO 13485:2016, *Medical devices – Quality management systems – Requirements for regulatory purposes*
- EN ISO 14971:2012, *Medical devices. Application of risk management to medical devices*
- PD ISO/TR 24971:2013, *Medical devices. Guidance on the application of ISO 14971*
- EN IEC 62304:2006, *Medical device software – Software life cycle processes*
- EN ISO IEC 62366-1:2015, *Medical devices – Part 1: Application of usability engineering to medical devices*
- IEC ISA 62443 series, *Industrial communication networks – Network and system security*
- ISO IEC 27005:2011, *Information technology – Security techniques – Information security risk management*
- ISO IEC 27032:2012, *Information technology – Security techniques*
- ISO IEC 80001 series, *Application of risk management for IT-networks incorporating medical devices*
- EN IEC TR 80002-1:2009, *Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software*
- ISO DTR 80002-2, *Medical device software – Part 2: Validation of software for medical device quality systems*
- IEC TR 80002-3:2014, *Medical device software – Part 3: Process reference model of medical device software life cycle processes (IEC 62304)*
- EN IEC TR 80001-2-8:2016, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*
- IEC 82304-1:2016, *Health software – Part 1: General requirements for product*

References

1. P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices: Evidence and Research*, pp. 305–315, 20 July 2015.
2. NIB, "Personalised Health and Care 2020 – Work Stream 1.2 RoadMap," National Information Board, June 2015.
3. KPMG, "Health care and cyber security – increasing threats require increased capablities," KMPG, 2015.
4. Independent Security Evaluators, "Securing Hospitals," 23 Feburary 2016. [Online]. Available: https://securityevaluators.com/hospitalhack/securing_hospitals.pdf. [Accessed 11 September 2016].
5. TrapX Labs, "Anatomy of an attack Medjack (Medical Device Hijack)," May 2015. [Online]. Available: http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf. [Accessed 7 August 2016].
6. National Data Guardian for Health and Care, "Review of Data Security, Consent and Opt-Outs," National Data Guardian, 2016.
7. K. Stouffer, V. Pillitteri, S. Lightman and M. Abrams, "NIST SP 800-82R1 Guide to Industrial Control Systems (ICS) Security," National Insititute of Standards and Technology (NIST), 2013.
8. K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, "NIST SP 800-82R2 Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, 2015.
9. FDA, "MAUDE Adverse Event Report: Merge Healthcare Merge Hemo Programmable Diagnostic Computer February 201," 02 August 2016. [Online]. Available: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi__id=5487204. [Accessed 07 August 2016].
10. FDA, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication," 09 January 2017. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. [Accessed 23 January 2017].
11. John Woodrow Cox, "MedStar Health turns away patients after likely ransomware cyberattack," *The Washington Post*, 29 March 2016. [Online]. Available: https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html. [Accessed 29 January 2017].
12. ICS-CERT, "Hospira LifeCare PCA Infusion System Vulnerabilities (Update B)," 10 June 2015. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B. [Accessed 07 August 2016].
13. J. Radcliffe, "R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump," Rapid7, 04 October 2016. [Online]. Available: https://community.rapid7.com/community/infosec/blog/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump. [Accessed 16 October 2016].
14. FDA, "Postmarket Management of Cybersecurity in Medical Devices," 27 December 2016. [Online]. Available: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf. [Accessed 22 January 2017].
15. EN ISO 14971: 2012: Medical Devices – Application of Risk Management to Medical Devices.
16. CVE, "Common Vulnerabilities and Exposures," 2016. [Online]. Available: https://cve.mitre.org/.
17. T. Bonaci and H. J. Chizecky, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics," *ACM Transaction on Cyber-Physical Systems*, pp. 1–11, 2016.
18. R. Piggin, "Developments in industrial robotic safety," *Industrial Robot: An International Journal*, vol. 32, no. 4, pp. 303–311, 2005.
19. AAMI TIR57:2016 Principles for medical device security – Risk management
20. ISA, "NIST Cybersecurity Framework ISA99 Response to Request for Information," ISA, 2013.
21. R. Piggin, "Process safety and cyber security convergence: Lessons identified, but not learnt?," in *8th IET International Conference of System Safety, incorporating the Cyber Security Conference*, 2013.

22. R. S. H. Piggin and H. A. Boyes, "Safety and security – a story of interdependence," in *IET System Safety and Cyber Security Conference 2015*, Bristol, 2015.

23. Allen & Overy, "Cybersecurity in life sciences:what is your duty of care?," 26 July 2016. [Online]. Available: http://www.allenovery.com/publications/en-gb/Pages/Cybersecurity-in-life-sciences-what-is-your-duty-of-care.aspx. [Accessed 20 August 2016].

24. NHS Digital, "SCCI0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems – Specification," NHS Digital, 2016.

25. NHS Digital, "SCCI0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems," NHS Digital, 2016.

26. Department of Homeland Security (DHS), "Cyber Security Procurement Language for Control Systems," 09 September 2016. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf. [Accessed 28 August 2016].

27. FDA, "Medical Device Single Audit Program (MDSAP) Pilot," 09 September 2016. [Online]. Available: http://www.fda.gov/MedicalDevices/InternationalPrograms/MDSAPPilot/ucm377578.htm. [Accessed 11 December 2016].

28. Department of Energy, Department of Homeland Security, "Cyber security capability maturity model (C2M2)," 21 March 2014. [Online]. Available: http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf. [Accessed 5 November 2016].

29. BSIMM, "BSIMM Framework," 10 December 2016. [Online]. Available: https://www.bsimm.com/framework/. [Accessed 10 December 2016].

30. R. Piggin, "Protecting Critical Systems," *ITNOW*, vol. 53, no. 1, pp. 10-13, December 2010.

BSI is grateful for the help of the following people in the development of the white paper series.

Author

Dr Richard Piggin, Security Consultant, Atkins

Richard is a security consultant at Atkins. He has an Engineering Doctorate in industrial networking from the University of Warwick and is both CISSP (information systems security) and GICSP (industrial cybersecurity) certified. His career has focused upon aspects of networking, including technology adoption, international standards, safety and security. Richard is a member of the IEC standards working group bridging safety and security. He also chairs the IET Cybersecurity Technical Professional Network. Richard is working with clients to make their Operational Technology resilient against current and emerging threats.

Expert Reviewers

Valerie Field, Interim Group Manager, Devices Regulatory Group , MHRA

Valerie Field qualified as a Diagnostic Radiographer in Nottingham and held many clinical and managerial posts in the National Health Service before working in the private healthcare sector. Following this Valerie held posts with the then National Care Standards Commission and the Health Care Commission before joining the MHRA in 2004. Valerie has held a range of roles at MHRA and is currently the Interim Group Manager for the Devices Regulatory group. She is the lead for the fast developing software apps area. She was a member of the programme board on the National Information Board's [NIB] 'Personalised Health and Care 2020' framework group looking at Healthcare apps. In 2014 she coordinated and input to the production of the first MHRA 'Guidance on medical device stand-alone software (including apps)' and again in August 2016 oversaw the publication of the new updated interactive version of the guidance.

Francisco J. Gomez-Rincon, ICS/SCADA Cyber Security Consultant, PwC

Francisco is CISSP certified security consultant for PwC's Cyber Security team for Energy, Utilities, Mining and Industrial Products. He has over 17 years of experience in the fields information assurance, cyber security, project management and software engineering. He specialises in information security assessments, network and security architecture assessments for industrial control systems and design and deployment of risk mitigation technology for critical infrastructure.

Aneela Lala, Certification Lead, Active Devices, BSI Healthcare

Aneela is a qualified electronics engineer with over 16 years of experience in the medical devices industry, including 4 years of research and development at the University of Auckland Bioengineering Institute, 6 years of manufacturing, service and support at leading medical device manufacturers and 6 years of regulatory experience. Aneela is Certification Lead, Scheme Manager and Technical Expert for the Active Devices team at BSI Healthcare and is experienced in auditing to the Medical Device Directive 93/42/EEC. In addition she is a BSI trainer for the MDD 93/42/EEC, ISO 14971 Risk Management, Post Market Surveillance and Vigilance, EN 62304 Medical Device Software and Technical File Writing.

Eugene Malinskiy, CEO and co-Founder, Infinite Arthroscopy Inc.

Eugene is steeped in the world of medical devices, cutting edge research, and compassionate innovation that looks to make the world a better place. Delivering medical device projects for external clients in areas as diverse as orthopaedics, cardiology, neurology, and wearable devices he was named to 2015 Forbes' 30 Under 30 in Manufacturing & Industry. Currently working on novel in-house breakthrough innovations for orthopaedics and other specialties. Past work has covered areas as diverse as IT networking and security, pharmaceuticals, and emergency medical services. Education background includes chemistry, biochemistry, EMT, biomedical engineering, internal comparative medicine, and other applied research fields.

Colette McIntyre, GCP/GLP Specialist, HeartSine Technologies, a division of Physio-Control, Inc.

Colette graduated from the University of Newcastle Upon Tyne with a BSc (Hons) in Microelectronics and Microprocessor Applications. Since graduating, she has held a number of quality assurance and quality management roles in the medical device, telecommunications and automotive industries and has acquired over 25 years of experience in quality management and auditing. Colette's current role is GLP/GCP Specialist with HeartSine Technologies where her main responsibilities include development of SOPs for the R&D department including GLP/GCP SOPs, design control and risk management; ensuring regulatory compliance for non-clinical and clinical studies and risk management activities during product development.

Dr Basil Yannakoudakis, Coordinator and Analyst, Devices Clinical Team, MHRA

Basil graduated in microbiology and then completed an MRes in Experimental Animal Physiology and Drug Discovery at Imperial College, London. He then went on to complete a PhD in Developmental Biology at King's College, London. Currently Basil serves as a Coordinator and Analyst for the Devices Clinical Team at MHRA. In this role he carries out research to support the Devices Safety and Surveillance Group, the European Regulatory Affairs Group and Expert Advisory Groups. Basil sits on a variety of cross-divisional teams including the Software Group and is also heavily involved with external clinical engagement.

Advisory Panel

Jane Edwards, Global Product Manager, BSI

Jane holds a BSc in Chemistry and an MBA from Durham university. She has over 10 years' experience in the medical device industry, having previously worked for Coloplast in their ostomy and continence business. Jane's experience includes working within the pharmaceutical, chemical and telecoms industries for Glaxo Wellcome, ICI and Ericsson, allowing her to bring depth of knowledge from across many industries and technologies. Her current role in BSI allows her to work with technical reviewers across all disciplines ensuring that all BSI communications are accurate and relevant. She is a member of the European Medical Writers Association.

Leo Eisner, Principal consultant of Eisner Safety Consultants

Leo's firm specializes in helping clients through product safety, international regulatory and quality system processes. Leo is a Notified Body Auditor for NEMKO (previously for NSAI & TÜV PS). Leo is the convener of IEC SC62D JWG9 (IEC/ISO80601-2-58) & a committee member of US TAG for TC62, SC62A & SC62D. Leo is a registered professional engineer in safety and has 28 years' experience in product safety. Leo is a member of RAPS, AAMI, ASQ, & IEEE. He's manager of the LinkedIn discussion group IEC 60601 Series – Medical Electrical Equipment.

Pete Philips, Director of the Surgical Materials Testing Laboratory (SMTL)

Pete is the Director of the Surgical Materials Testing Laboratory (SMTL), based in Bridgend in South Wales, which is funded by the Welsh Government to test medical devices for the Welsh NHS and to provide technical advice on medical devices. He has worked in the medical devices field for 30+ years, and sits on a number of BSI, CEN and ISO medical device committees and groups. He chairs the Welsh Non-Luer Connectors Reference Group (WNCRG) for Welsh Government, which is coordinating the implementation of new ISO compliant non-Luer connectors across the Welsh NHS, and represents Welsh Government on medical devices on various other groups.

Published white papers

The Proposed EU Regulations for Medical and In Vitro Diagnostic Devices: An Overview of the Likely Outcomes and Consequences for the Market, Gert Bos and Erik Vollebregt

Generating Clinical Evaluation Reports – A Guide to Effectively Analysing Medical Device Safety and Performance, Hassan Achakri, Peter Fennema and Itoro Udofia

Effective Post-market Surveillance – Understanding and Conducting Vigilance and Post-market Clinical Follow-up, Ibim Tariah and Rebecca Pine

What You Need to Know About the FDA's UDI System Final Rule, Jay Crowley and Amy Fowler

Engaging Stakeholders in the Home Medical Device Market: Delivering Personalized and Integrated Care, Kristin Bayer, Laura Mitchell, Sharmila Gardner and Rebecca Pine

Negotiating the Innovation and Regulatory Conundrum, Mike Schmidt and Jon Sherman

The Growing Role of Human Factors and Usability Engineering for Medical Devices: What's Required in the New Regulatory Landscape? Bob North

ISO 13485: The Proposed Changes and What They Mean for You, Bill Enos and Mark Swanson

The Differences and Similarities between ISO 9001 and ISO 13485, Mark Swanson

How to Prepare for and Implement the Upcoming MDR: Dos and Don'ts, Gert Bos and Erik Vollebregt

How to Prepare for and Implement the Upcoming IVDR: Dos and Don'ts, Gert Bos and Erik Vollebregt

Planning for Implementation of the European Union Medical Devices Regulations – Are you prepared?, Eamonn Hoxey

Forthcoming white papers

The European Medical Devices Regulations: What are the requirements for vigilance reporting and past-market surveillance?, Eamonn Hoxey

Medical Device Market Surveillance Requirements: Are you aware of your responsibilities? (working title)

Clinical Data – Away from Clinical Equivalence in Europe (working title)

General Requirements for Safety and Performance (working title)

Modifying, Creating and Maintaining Technical Documentation (working title)

About BSI Group

BSI (British Standards Institution) is the business standards company that equips businesses with the necessary solutions to turn standards of best practice into habits of excellence. Formed in 1901, BSI was the world's first National Standards Body and a founding member of the International Organization for Standardization (ISO). Over a century later it continues to facilitate business improvement across the globe by helping its clients drive performance, manage risk and grow sustainably through the adoption of international management systems standards, many of which BSI originated. Renowned for its marks of excellence including the consumer recognized BSI Kitemark™, BSI's influence spans multiple sectors including aerospace, construction, energy, engineering, finance, healthcare, IT and retail. With over 70,000 clients in 150 countries, BSI is an organization whose standards inspire excellence across the globe.

BSI is keen to hear your views on this paper, or for further information please contact us here:
julia.helmsley@bsigroup.com

This paper was published by BSI Standards Ltd

For more information please visit:
http://www.bsigroup.com/en-GB/our-services/medical-device-services/BSI-Medical-Devices-Whitepapers/

BSI Group Headquarters
389, Chiswick High Road
London W4 4AL
United Kingdom

T: +44 (0) 845 086 9001
E: cservices@bsigroup.com
bsigroup.com

BSI UK
Kitemark Court
Davy Avenue
Knowlhill
Milton Keynes MK5 8PP
United Kingdom

T: +44 (0) 845 080 9000
E: MK.customerservices@bsigroup.com
bsigroup.com

BSI Group America Inc
12950 Worldgate Drive
8th Floor Monument II
Herndon
VA 20170
USA

T: +1 800 862 4977 / 703 437 9000
E: inquiry.msamericas@bsigroup.com
bsiamerica.com