# Smart Hospitals

## Security and Resilience for Smart Health Service and Infrastructures

NOVEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Contact

For contacting the authors please use eHealthSecurity@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

## Acknowledgements

Julio Mayol, Hospital Clinico San Carlos
Andrea Zapparoli Manzoni, KPMG Advisory S.p.A
Franck Calcavecchia, Geneva hospital
Yordan iliev, CIO, National Oncology Hospital
Dr. Björn Kabisch, Jena University Hospital
Christian Lovis, University Hospitals of Geneva and University of Geneva
Maik Morgenstern, AV-TEST GmbH
Rui Gomes, Portuguese Ministry of Health
Götz Gerald, Munich Municipal Hospital Ltd
Dr. Dimitrios Glynos, CENSUS S.A.
Spyridon Antonatos, IBM Research Ireland.
Greg Fletcher, NHS Digital
Pia Jespersen, National eHealth Data Authority


ISBN 978-92-9204-181-6, doi: 10.2824/28801

# 1 Table of Contents

# Executive Summary

In recent years, many pervasive systems for healthcare have been proposed, discussed and sometimes realised. Pervasive healthcare is highly multifaceted, with many applications focusing on interoperability with the legacy hospital assets, the "traditional hospital", the security and privacy of sensitive information and the usability of end users. The notion of smart hospitals is introduced when Internet of Things (IoT) components are supporting core functions of a hospital. Collaboration among various stakeholders, numerous interconnected assets and high flexibility requirements do not only lead to complexity and dynamics but also to blurred organisational boundaries. Due to the great number of significant assets at stake (patient life, sensitive personal information and financial resources) information security is a key issue for smart hospitals.

Threats to smart hospitals are, however, not limited to malicious actions in terms of their root cause. Human errors and system failures as well as third-party failures also play an important role. The risks that result from these threats and corresponding vulnerabilities are typically mitigated by a combination of organisational and technical security measures taken by smart hospitals which comprise good practices. With respect to organisational measures, compliance with standards, staff training and awareness raising, a sound security organisation, and the use of guidelines and good practices are particularly relevant. Relevant technical measures include network segmentation, asset and configuration management, and network monitoring and intrusion detection. However, manufacturers of information systems and devices used in smart hospitals have to take certain measures too. Among them are, for instance, building security into products from the outset, adopting secure coding practices and extensive testing.

Based on the analysis of documents and empirical data, and the detailed examination of attack scenarios found to be particularly relevant for smart hospitals, the study proposes key recommendations primarily for hospital executives. Namely hospitals should:

- Establish effective enterprise governance for cyber security
- Implement state-of-the-art security measures
- Provide specific IT security requirements for IoT components in the hospital
- Invest in NIS products
- Establish an information security sharing mechanism
- Conduct risk assessment and vulnerability assessment
- Perform penetration testing and auditing
- Support multi-stakeholder communication platforms (ISACs)

The study also makes recommendations for industry representatives in order to enhance the level of information security in smart hospitals. Namely industry players should:

- Incorporate security into existing quality assurance systems
- Involve third parties (healthcare organisations) in testing activities
- Consider applying medical device regulation to critical infrastructure components
- Support the adaptation of information security standards to healthcare

# 1 Introduction

The “Internet of things” is a revolution for the ICT world. Devices, system components and networks are becoming autonomous, ubiquitous and interconnected. When this technological advancement applies to the healthcare sectors, one of the most traditional critical sectors[1] , the results are remarkable. Connected medical devices transform the way the healthcare industry works, both within hospitals and between different actors of the healthcare industry. Could you imagine an electronic device collecting information on patients’ vital signs becoming “smart”? Or one that monitors life supporting machines to be able to react on any change of status? Connected medical devices can bring increased patient safety and efficiency, particularly if connected to Clinical information systems. When this applies to the whole healthcare organisation ecosystem, it becomes a “Smart Hospital”.

However, the increased flow of information within and between hospitals brings risks that C-level professionals in the hospital (CIO, CISO etc.) need to address. The risks include possible harm to patient safety or loss of personal health information and may not only be caused by malicious actions but also by human errors, system or third-party failures and natural phenomena. As the attack surface increases with the introduction of connected devices, the attack potential grows exponentially.

## 1.1 Objective and scope

The objective of this study is to improve information security and resilience of hospitals to prevent disruptions to smart components that can cause greater impact to patients’ safety. The ultimate goal is to offer enhanced patient safety.

This study investigates the current status of Smart Hospitals and related information security issues, focusing on deployments in the EU. This involves determining the objectives achieved through “smart” devices and systems, the assets that make up a Smart Hospital, the information security threats as well as the security measures available to address them. Through gap identification between current threats and existing measures, this study makes concrete recommendations to improve information security in smart hospitals.

The focus of the study is the hospital itself and specifically on all the smart components that are offering value when built on top of already existing traditional systems, see Figure 1 .

[1] http://www.csihshow.co.uk/

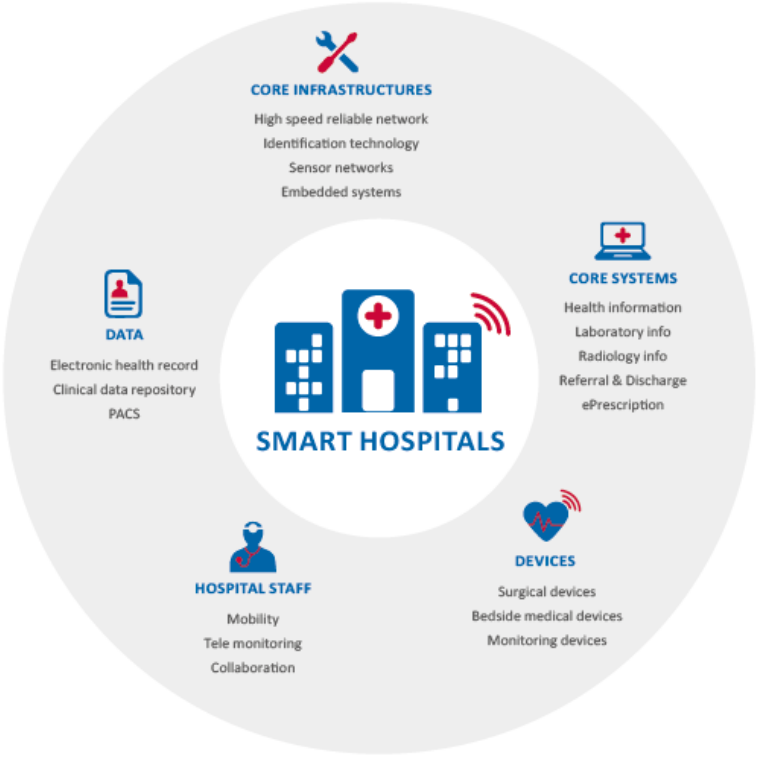


**Figure 1 Study perimeter: Traditional Hospital**

## 1.2 Methodology

This report was developed using a combination of desktop research as well as information from interviews with key stakeholders. The document analysis focuses on scientific, as well as industry and policy material, related to information security in smart hospitals. The interviews and the survey were conducted to validate and extend the findings of the document analysis.

The approach taken follows the ENISA methodology[2] developed over the last three years based on the ENISA threat landscape approach, and involved:

- Mapping assets and developing a threat taxonomy that covers possible attacks via desktop research, and validating or identifying further gaps through interviews with security experts working in the field of healthcare information security, focusing on Hospitals.
- The assets are categorised based on their criticality, meaning the impact an incident in one of these could cause.
- Enumerating possible attacks that target or affect smart components in hospitals.
- Developing three attack scenarios with mitigation actions to provide information on practical examples of implementation, and validating these with security experts working in Hospitals.
- Developing good practices and performing a gap analysis based on desktop research and interviews.
- Proposing recommendations for future steps in information security for Smart Hospitals in Europe.

[2] The term "asset" has two slightly different meanings in the information security context. In some cases the term is used to refer to the mostly technical components of an organisational information system. Such components allow organisations to meet their objectives but differ from each other with regard to their criticality. In other cases, the term is used more broadly to refer to organisational values that need to be protected. The protection of such values is sometimes an objective in itself.

Thirty experts participated in the interviews and the survey. Participants were hospital representatives, industry representatives and policy makers. Figure 2 depicts the distribution of participants across the three groups. All were able to draw on several years of experience with Information and Communication Technology (ICT) in healthcare and held senior positions.

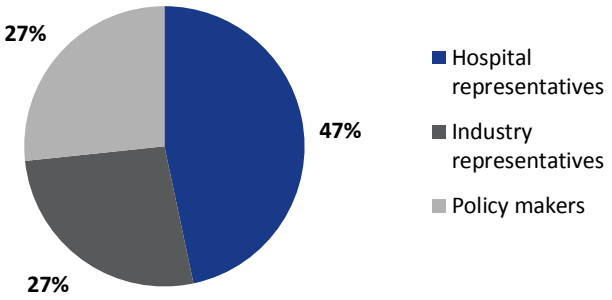


**Figure 2 Distribution of respondents**

## 1.3 Target Audience

The target audience of this study is executives and C-level professionals from hospitals. The aim is to help them to understand which are the steps they need to take to ensure information security when choosing "smart" solutions. IT and security professionals are of particular relevance (e.g. Chief Medical Information Officers, Chief Information Security Officers (CISOs)).

As a secure "Smart hospital" design has extensions to devices and systems security, this document could be useful also (but not only) for:

- Industry representatives: Executives and professionals of manufacturers of connected devices for healthcare are relevant with respect to industry representatives as well as technology and consulting companies focused on information security.
- Policy makers: Policy makers from Member States and the European Union (EU) are relevant if they are in charge of policies dealing with healthcare, critical infrastructures or information security.

## 1.4 Structure

The study is structured as follows:

- Section 2 describes the smart hospital environment, paying particular attention to the definition of the term, the regulatory framework and guidelines related to information security, the objectives hospitals pursue and the effect of being "smart" on these objectives, and the key assets to be protected.
- Section 3 pursues an asset-centric approach to threat and risk analysis. Based on the key assets and a vulnerabilities, potential attack points and threat types are discussed.
- Section 4 describes five attack scenarios ranging from social engineering attacks on hospital staff to distributed denial-of-service attacks on hospital servers.
- Section 5 describes the control and recovery measures available to protect the smart hospital from the threats faced. A differentiation is made between measures to be implemented by hospitals and the industry, respectively.
- Section 6 makes concrete and actionable recommendations aimed at hospital executives, industry representatives and policy makers. Additionally, examples of good practice are described.

# 2 Smart Hospitals

This section is split in two parts. The first part describes the smart hospital environment, placing emphasis on the definition of the term "smart hospital", the objectives of introducing "smartness" in a hospital environment, the guidelines related to information security and the respective regulatory framework. The second part focuses on the assets that introduce "smartness" in the hospital environment and need to be protected due to their criticality for the operation of smart hospitals.

## 2.1 The Smart Hospital Environment

The overarching goal of smart hospitals is to deliver optimal patient care by making the most of advanced ICT. The availability of all relevant information when required; access to internal and external expertise when needed; and efficient and effective surgical/diagnosis processes that facilitates achieving this goal with low error rate and cost effectively.

A **definition** of the term "smart hospitals" may thus be:

> "A smart hospital is a hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities".

What makes a hospital smart is, therefore, the availability and use of meaningfully interconnected systems and devices that lead to overall smartness. While legacy systems may indeed be an integral part of end-to-end smart processes, the emphasis of this study will be on new technologies, and particularly IoT components.

In this document, the term "traditional hospital" is used to refer to hospitals that do not fall into the group of smart hospitals as defined above. The motivation behind moving to a smart hospital environment comprising optimised / automated end-to-end processes and IoT components is based on the improvement of existing hospital processes and the introduction of new capabilities in patient healthcare. However this migration comes with increased challenges related to the extended reliance on ICT. These two combine to define the **Objectives** of a smart hospital, depicted in Figure 3.

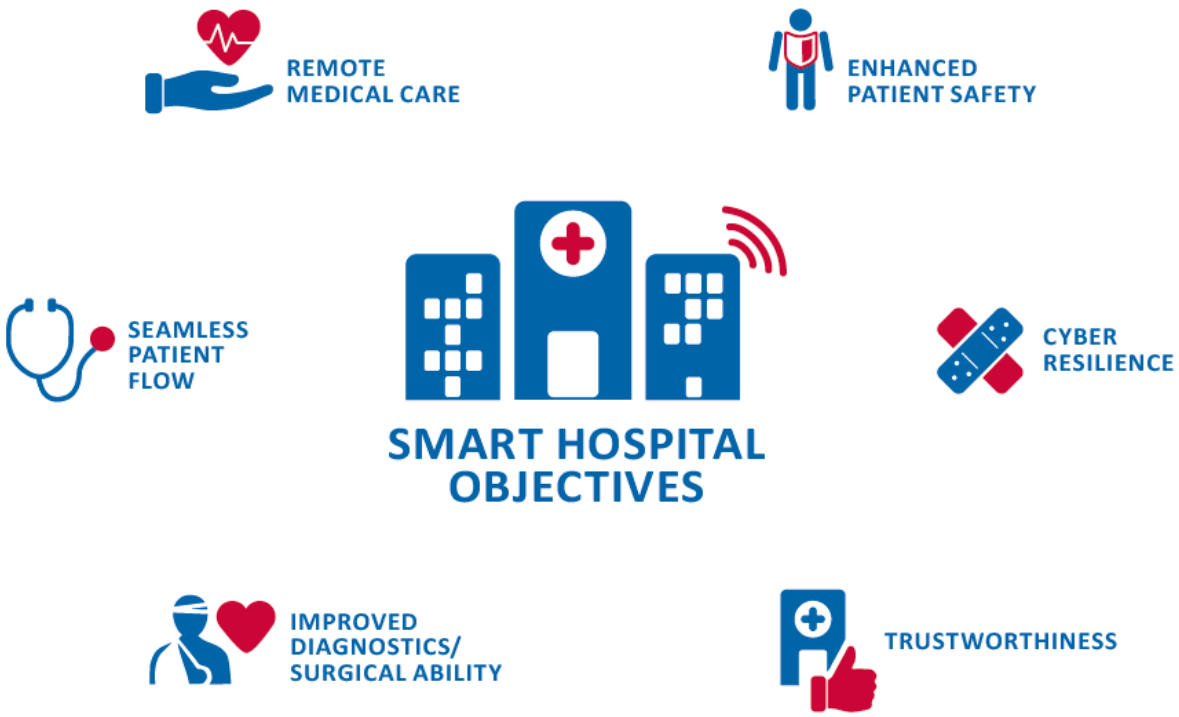


**Figure 3 Smart Hospital Objectives**

As detailed below, type and extent of ICT usage significantly affects the objectives as well as related challenges and opportunities:

- Improved diagnostics / surgical ability: ICT does not only enable new treatment methods (e.g. surgical robots can perform micro-surgery, which cannot be done by clinicians) but can also improve existing methods. Hospitals are increasingly able to mine patient data to help with diagnosis or choosing the best course of treatment, and sophisticated software solutions are allowing them to fine-tune their administrative processes.
- Seamless patient flow: Efficient healthcare as well as efficient patient flow can reduce waiting times and the duration of hospital stays, reduce errors, increase revenues and boost patient (and employee) satisfaction. ICT can be deployed to identify, analyse and resolve bottlenecks and thereby contribute to efficient healthcare and patient flow. In smart hospitals, efficient healthcare and efficient patient flow may, for instance, be supported by automatic updates of medical information across networked devices and information systems. The resulting availability of patient information in all stages - from entry to exit – and the optimisation of admission, scheduling and other processes around it result in seamless patient flow.
- Remote medical care: One of the key objectives of introducing IoT devices in the healthcare context is the ability to extend the hospital borders and provide remote medical care. Various medical devices, e.g. implantable devices, wearable devices and other mobile devices introduce the ability to perform real-time patient monitoring through measurement of key vital signs and make these measurements readily available to hospital staff and systems via network connections. These remote patient care capabilities are augmented by several medical devices that offer the ability to act (e.g. administer a medical dose) on the patient depending on status or via remote controls. Hence, patient admission to hospitals can be limited to

those cases deemed necessary, resulting in reduced patient care costs and improved patient experience, as the patient can now receive treatment from his/her own home.

- Enhanced patient safety: Enhancing healthcare delivery and patient flow also increases patient and clinical safety. It is important though that healthcare delivery and patient flow do not improve at the expense of safety. Without doubt, properly used, devices collecting data about patient vital signs and medication intake, or monitoring life support machines, can lead to increased patient safety if they are connected and able to provide timely warning.
- Cyber Resilience: Cyber Resilience refers to the ability of a hospital to ensure the availability and continuity of its services that rely on ICT assets. Higher ICT penetration inevitably leads to greater ICT dependency, which, in turn, increases the relevance of information security for smart hospitals. In some European countries, the health sector is considered a critical infrastructure to be particularly protected[3]. Healthcare actors including hospitals need to anticipate, prepare for, and respond and adapt not only to incremental change but also to sudden disruption. In smart hospitals, achieving this is more challenging than in traditional hospitals because the number of components that could lead to and be affected by service unavailability is much higher.
- Trustworthiness: Being perceived as trustworthy and having a good reputation is a competitive issue in areas where choosing between different providers is an option. Trustworthiness also affects adherence to medications and continuity of care, which has implications for the outcomes a hospital can achieve. Being at the forefront in terms of ICT usage clearly provides reputational advantages. At the same time, patient safety and privacy must not be put in jeopardy to avoid damaging reputation.

The survey respondents confirmed that with respect to all objectives presented above hospitals benefit from an IoT implementation. Every single participant stated, for instance, that an IoT implementation results in additional opportunities regarding patient/clinical safety and almost three quarters of the respondents expected benefits for resilience.

With respect to the **regulatory framework**, national information security and e-health strategies, as well as related legislation, are of particular relevance. Neither of them, however, pays particular attention to the specifics of smart hospitals. Nevertheless, these documents need to be taken into account by hospital executives and industry representatives.

There are several white papers, mainly provided by industry representatives (manufacturers of medical devices as well as technology and consulting companies focused on information security such as IBM[4], Symantec[5], Deloitte[6] or ReedSmith[7]), which may serve as rough guidelines for hospital executives. However, they typically do not go into detail when it comes to specific threats faced by smart hospitals and relevant security measures.

[3] THREATS: An Analysis of Critical Infrastructure Protection Measures Implemented within the European Union: Identifying which European Union Member States includes the Health Sector as part of Critical National Infrastructure and which facets of Health Infrastructure are considered Critical, http://www.threatsproject.eu/WP1%20D1%20final.pdf, 2014.

[4] IBM Global Business Services: The Digital Hospital Evolution: Creating a Framework for the Healthcare System of the Future, https://www.ibm.com/smarterplanet/global/files/whitepaper_-_the_digital_hospital_evolution.pdf, 2013.

[5] Symantec: An Internet of Things Reference Architecture, https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-wp-en.pdf, 2016.

[6] Deloitte: Networked Medical Device Cybersecurity and Patient Safety: Perspectives of Health Care Information Cybersecurity Executives, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf, 2015.

[7] ReedSmith: Cybersecurity for Medical Devices: A Risk Mitigation Checklist for In-House Counsel, https://www.reedsmith.com/files/Publication/65d1e359-2168-44e9-9b78-980ea2ebc0e8/Presentation/PublicationAttachment/45e57ded-d467-40e9-a2fa-9d3895d63788/alert15247.pdf, 2014.

The International Organisation for Standardisation (ISO) published several standards focusing on health informatics. IEC 80001-1[8], for instance, which deals with the application of risk management to networks incorporating medical devices, provides the roles, responsibilities and activities necessary for risk management, and is particularly relevant in the context of smart hospitals and information security. ISO also published a series of technical reports with different emphasis, which provide guidance for the implementation of IEC 80001-1. The ISO/IEC 2700x series of standards, which deals with information security management, is relevant for smart hospitals as well as for all types and sizes of organisations.

New medical systems and devices need to be classified according to their risk before they can be certified and conformity with the Medical Devices Directive[9] (MDD), the In Vitro Diagnostic Device Directive[10] (IVD) or the Active Implantable Medical Device[11] (AIMD) Directive can be confirmed. Conformity with the MDD is also applicable to certain ICT products used in hospitals meaning that this can have implications to the use of any "smart" device in a hospital.

[8] http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863
[9] https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en
[10] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0079
[11] https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/implantable-medical-devices_en

## 2.2 Assets

### 2.2.1 Overview of Smart Hospital Assets

Hospitals have a wide range of assets that are essential for their operation and thus need to be protected. While some smart hospital assets are also relevant in traditional hospitals, others are quite characteristic of smart hospitals since they are intelligently connected and able to take decisions autonomously. Among these assets are, for instance, mobile client devices, identification systems and interconnected clinical information systems. The specific assets that characterise smart hospitals are at the focus of this section.

1. **Remote care system assets** comprise the ICT ecosystem that allows the smart hospital to extend its borders and provide healthcare services to patients at remote locations (e.g. at home):

    - medical equipment for tele-monitoring and tele-diagnosis (e.g. measurements of blood pressure, heart rate, glucose measurements, ECG and other remote physiological measurements, threshold-triggered alarm generators etc.), such equipment may take the form of wearable or implantable devices etc. ;
    - medical equipment for distribution of drugs (automated dosing equipment) or to administer treatment;
    - telehealth equipment, such as cameras, sensors and telephone/internet connections; telehealth computer system for patients to register their physiological measurements themselves (including patient-side application/software if applicable)

2. **Networked medical devices** whose extensive use typically characterises smart hospitals and also enable remote patient monitoring, which is a key service that smart hospitals can provide to healthcare management at a national level, compared to traditional hospitals. Moreover, modern implantable devices such as pacemakers can be updated, reducing the number of reasons for replacement. Stationary as well as mobile devices have also been used a lot in traditional hospitals. In the smart hospital context, however, they are intelligently connected with identification components and clinical information systems increasing the automation level and the decision making ability. Examples include:

    - mobile devices (e.g. glucose measuring devices)[12];
    - wearable external devices (e.g. portable insulin pumps, wireless temperature counters);
    - implantable devices (e.g. cardiac pacemakers);
    - stationary devices (e.g. computer tomography (CT) scanners, life support machines, chemotherapy dispensing stations);
    - supportive devices (e.g. assistive robots).

3. **Identification systems** are used to track and authenticate patients, staff or hospital equipment such as beds. In smart hospitals, the biometric scanners do not only read the identification systems but are also intelligently networked with devices and information systems. Moreover, closed-circuit security systems play a key role regarding authentication – and subsequently also authorisation (e.g. allowing access to specific areas) – in smart hospitals. Examples include:
    - Identification systems items such as tags, bracelets, labels and smart badges (e.g. ultrasound-enabled);
    - Biometric scanners;

[12] The devices categorised as remote care provision devices can also be used in the hospital as a networked medical device. However sometimes sophistication of the device is different (usability, data collection and analysis), this is why we separate in two categories.

- RFID systems with location services (software components) to assess and monitor relative movement of assets/patients/staff etc.;
- CCTV (video surveillance) with recognition/authentication capabilities

4. **Networking equipment** provides the connectivity backbone to support smart hospitals. The equipment required is not different than standard equipment used in a traditional hospital, but it is characterised by its enhanced features (e.g. routing protocols, bandwidth). Examples include:

   - Transmission media;
   - Network interface cards;
   - Backbone network devices (e.g. hubs, switches, routers etc.);
   - IoT Gateways which further analyse data collected by devices and send them to a data centre or the cloud

5. **Mobile Client devices** are intelligently integrated in smart hospitals to make the right information available at the right place at the right time and to facilitate mobility of staff and patients. Examples include:

   - Mobile clients (e.g. laptop computers, tablets, smartphones, pagers);
   - Mobile applications for smartphone and tablets;
   - Alarm and emergency communication applications for mobile devices.

6. **Interconnected clinical information systems** are deployed in smart hospitals jointly with medical devices and identification components to enable smart end-to-end patient care processes. Moreover, the clinical networked information systems in smart hospitals are increasingly able to take decisions autonomously. Examples include:
   - Hospital information systems (HIS);
   - Laboratory information systems (LIS);
   - Radiology information systems (RIS);
   - Pharmacy information system (PIS);
   - Pathology information system;
   - Blood bank system;
   - Picture archiving and communication systems (PACS);
   - Research information system.

7. **Data** are often considered important assets from an information security perspective. Mainly decisions a smart device will take is based on the analysis of collected data. Examples include:

   - Clinical and administrative patient data (e.g. health records, tests results, contact details);
   - Financial, organisational and other hospital data;
   - Research data (e.g. clinical trial reports) and data intended for secondary use;
   - Staff data;
   - Tracking logs;
   - Vendor details (e.g. contact details, products used).

8. **Buildings and facilities**, includeend-to-end smart processes that manage various functions are critical for the operation of smart hospitals. A number of crucial functions related to patient safety rely on the capabilities of intelligent facility management systems. Examples include:

   - Power and climate regulation systems, including smart ventilation systems;
   - Temperature sensors;

- Medical gas supply;
- Smart patient room operation and management systems, including smart boards, patient screens, medical staff screens etc.;
- Automated door lock system including smart locks (e.g. interconnected locks, wireless locks etc.), lock management applications/tokens (e.g. proximity unlocking via mobile device) and lock management software

An illustration providing an overview of the key assets is depicted in Figure 4.

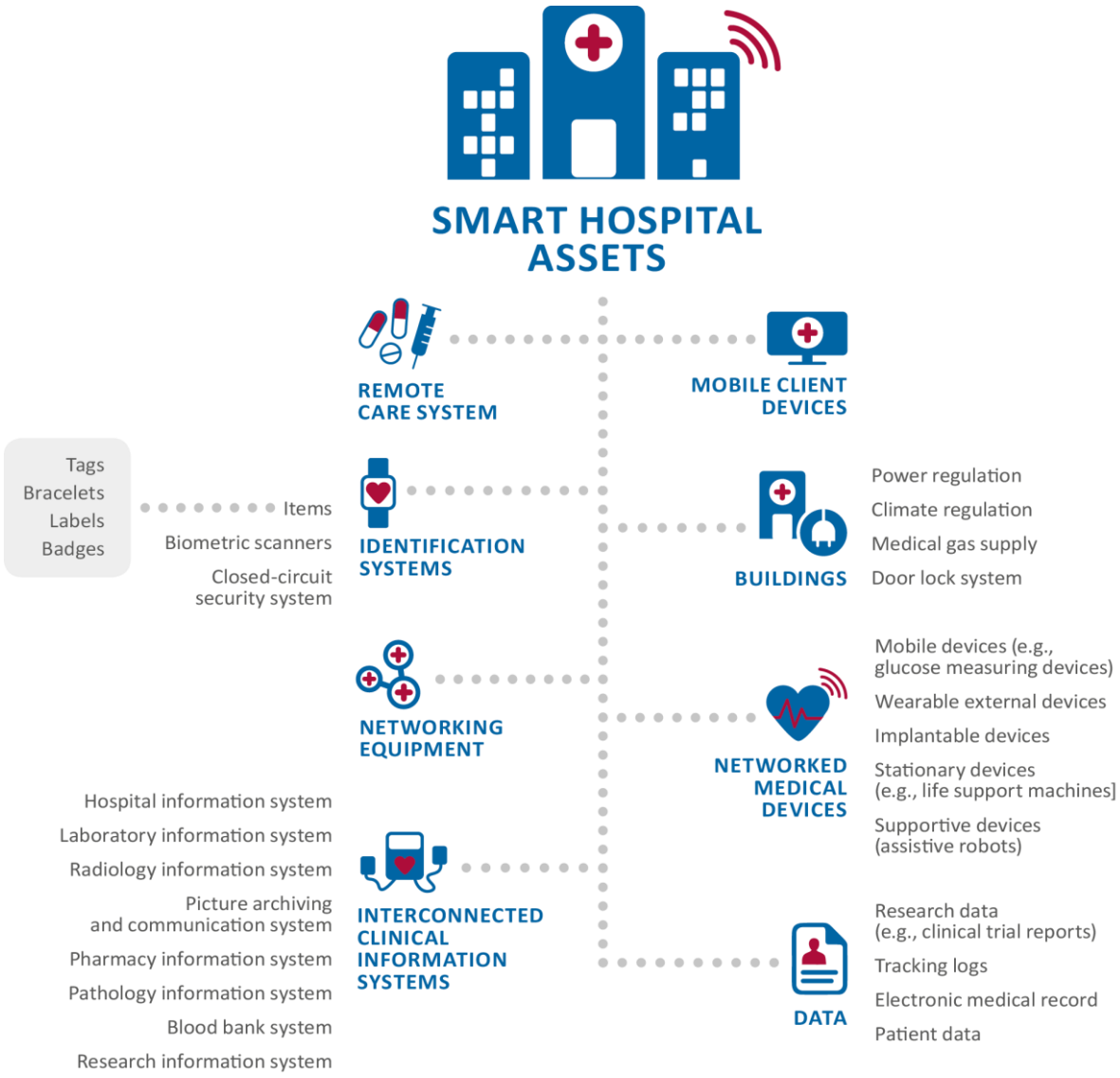


**Figure 4 Smart Hospital Assets**

### 2.2.2 Criticality of Smart Hospital Assets

In this large ecosystem called smart hospital, not all assets have the same criticality for the normal operation and service offering. An asset is designated as critical when any interruption or malfunction would have great impact to the operation of the overall system but also to the patients. The assets as presented above were assessed based on the impact any interruption of their service could cause, namely their criticality.

Figure 5 depicts which assets are considered most critical for the operation of a smart hospital, based on empirical data collected during interviews and survey.

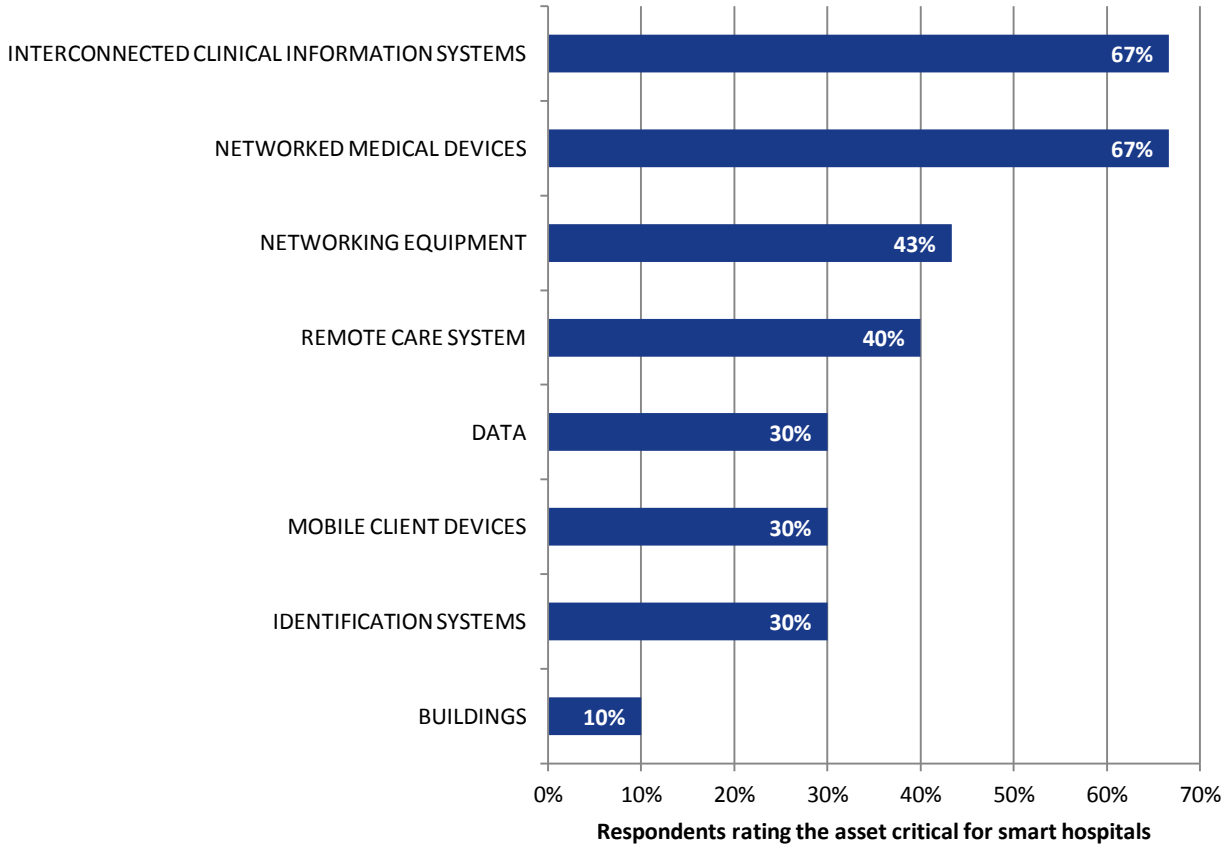


**Figure 5 Assets critical for smart hospitals**

The most critical smart assets in the context of a smart hospital are the interconnected clinical information systems and networked medical devices. This may be explained by the outstanding role they play in smart hospitals. The presence of intelligently connected clinical information systems and increasingly autonomous medical devices is among the most obvious changes during a hospital's digital transformation to a smart hospital. The achievement of many of the key objectives associated with smart hospitals depends strongly on the availability of reliable and networked clinical information systems and medical devices. Moreover, in order to achieve improved medical care and enhanced diagnostic capabilities, the IoT components and devices replace legacy systems that are of vital importance to the function of the hospital; this renders them directly critical not only for the patient safety but also for the overall hospital function.

Networking equipment is considered critical as it is the backbone of the Smart Hospital; without solid network architecture, increased capabilities in the context of bandwidth or interoperable solutions the IoT components wouldn't function properly. More specifically, information gathered by medical devices or end components needs to be analysed and combined with other medical information. This is typically held by the interconnected clinical information systems of the hospital as well as by third parties. Most of the analyses, however, are neither conducted by the medical devices nor by the clinical information systems but rather in a central system which is equipped with the technology to aggregate and analyse data from different internal and external sources efficiently. Networking is indispensable in order to get the data from the information systems and medical devices to this system taking the important decision (vital signs in a smart hospital room indicate the need of revision of the drug prescription).

One of the major objectives of the Smart Hospital is to be able to offer remote care services; to achieve this the hospital systems need to connect to the remote care systems at the patients' end. The difficulty that arises from this setting is that in case of a malfunction or a disruption the device/system will be restored by the respective vendor, as it falls outside the responsibility of the hospital. This explains the small rating in the criticality matrix, despite the importance of the data these system collect for diagnosis and drug prescription

Next in ranking come the data (research data, data logs etc), the mobile client services and the identification systems. Although these are very important assets for the functioning of a smart hospital, as they do not support the core functions (their use can span from awareness raising purposes to remote diagnosis or access) any disruption wouldn't cause a major outage to the provisioning of the hospital services.

Last in the ranking comes the building and facilities. In this case the impact of an interruption would occur is very big, however as the likelihood is very low (a "black swan" case, as per the official risk management term), it comes last in ranking. Studies, however, have shown that cyber-attacks targeting facility systems (climate regulation, power provision etc.) are not so common, since, on the one hand, they require high expertise and sophistication and, on the other, the result would not provide any financial benefit to the maleficent attacker (like in the case of ransomware).

# 3 Threat and risk analysis

## 3.1 Emerging vulnerabilities

This chapter details the most common vulnerabilities that need to be taken into account by smart hospitals. The list is not comprised only by technical vulnerabilities but extends to organisations and social aspects. Threats typically exploit vulnerabilities attributed to ICT assets and people. With respect to people, the most relevant groups are an organisation's staff and management. As the staff and management, respectively, procure, manage and operate ICT assets such as systems and devices, the two groups are closely related.

In general, security must be comprehensive; otherwise, attackers simply exploit the weakest link[13]. There are, however, several serious vulnerabilities that come with the use of IoT[14] in healthcare that are difficult to address. A key problem of smart hospitals is that personal health information is considered even more valuable than financial information by criminals. Apart from access to sensitive information, access to prescription drugs may also be considered worthwhile by attackers. When implementing IoT solutions the components are chosen for their low cost and specific capabilities; however, the capabilities are significantly below what might be justified when the assets protected are human life, and security costs may be a significant portion of the cost, or even greater than the cost of the components. Prevalent vulnerabilities, however, do not only facilitate malicious actions, they may also increase the likelihood and impact of human errors and system failures.

- IoT devices, including networked medical devices, are highly interconnected and some devices even have the ability to automatically connect to other devices. Consequently, security decisions made locally for a specific device can have global impacts[15]. In many cases medical devices were designed without the specific intent to be connected to a network (sometimes specifically intended to remain isolated) - that requirement came later and was bolted on. The communication between smart devices and legacy systems can also create gaps and give space for malicious attackers to gain illegal access to systems and data. The introduction of new components introduces a new attack surface.
- IoT devices are dispersed everywhere in the hospital (from sensors in the patient rooms to CCTV and RFID readers that provide access control). This means that physical security is practically impossible for all components. Protecting the perimeter is minimising this vulnerability however more protection is needed.
- Most medical device design intentionally avoids threat modelling activities. Devices are built based on "intended use" cases, and what a reasonable person might do. Hacking and other network-borne accidents are "unintended use" or "abuse" cases. This posture leads to a number of systemic vulnerabilities and risks throughout the healthcare ecosystem.
- There is a mass-scale deployment of homogeneous IoT devices, which makes it appear worthwhile to investigate viable attack paths. While device manufacturers and security companies need to remove all vulnerabilities, criminals only have to find one. It is virtually impossible to patch all vulnerabilities for all devices[16]. At the same time, however, if a specific vulnerably is removed, it is typically not very difficult for criminals to find another viable attack path.

[13] Symantec: An Internet of Things Reference Architecture, https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-wp-en.pdf, 2016.
[14] Internet Society: The Internet of Things: Understanding the Issues and Challenges of a More Connected World, https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf, 2015.
[15] Internet Society: The Internet of Things: Understanding the Issues and Challenges of a More Connected World, https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf, 2015.
[16] EY: Cybersecurity and the Internet of Things, http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf, 2015.

- Specifically for medical devices, their life span is a very important drawback to consider. Hospitals don't change CAT scanners or MRI machines every 3 years and when they buy the devices might already be outdated (it takes almost 3 years from design to testing and production of a medical device based on EU legislation). The same applies in the case of smart hospitals as usually IoT components are built on top of the already existing infrastructure.
- IoT devices run embedded operating systems and applications with little if any malware detection or prevention capabilities[17]. The small size and limited processing power of many connected devices often inhibits measures such as encryption or other robust security measures. Moreover, it is often difficult or impossible to reconfigure or upgrade devices.
- There is an increasing level of dependence on IoT devices, which are not known for being particularly resilient. Our dependence on connected technology is growing faster than our ability to secure it - in areas affecting human life and public safety a higher standard of care is warranted. This is particularly true for some medical devices that are vitally necessary for the survival of patients.
- The actual user has little or no insight into the internal functioning of the devices or the precise data streams they produce. With respect to medical devices, clinical staff, IT staff and the patient have little or no such insight. Risk decisions made by the manufacturer are not disclosed in any meaningful way to the healthcare provider, physician, or patient. This not only makes understanding potential threats but also reacting in a timely manner in case of an incident very difficult.
- There is often no clear way to alert the user when a security problem arises. This may result in a security breach that persists for a long time before being detected and remediated. It has already been shown, however, that compromised medical devices acted as bridgeheads for further malware proliferation in hospitals[18]. In healthcare this is especially important, because the traditional security mechanisms may "fail closed" by denying access - but that may put patient safety at risk more than "fail open" which grants full access.
- Access control is very important in the smart hospital environment as a lack of authorisation policy can cause unauthorised users to gain access through an end device to a critical system. Issues may be related to authentication or authorisation of staff that handles medical devices; in some cases the "need-to-know" basis or the understanding of the implications from cyber security perspective is missing.
- Despite being well-trained and aware, staff members may circumvent security measures such as policies and procedures if they are perceived as unnecessarily inconvenient or slowing them down[19]. In the hospital context, clinical staff may circumvent measures simply because of time pressure or because of conflicts with other objectives including efficient healthcare/patient flow, pleasant patient experience or patient/employee privacy.
- In a Smart environment, physicians or patients can make use of personal devices (mobile, wearables etc); lack of a clear and strict BYOD policy can be great vulnerability. Strengthening procedures compliant to the hospital's information security policy should be obligatory for the use of any external device. In many cases, the IT department is not even aware that such systems or devices are being used, while in other cases, the business need of introducing a new system/device to support the medical process does not allow sufficient time for proper testing of said system/device for compliance with the organisation's requirements.
- Due to clinical needs it is possible for systems or devices to be used that do not meet organisational or industry standards. In such cases, the IT department is usually aware of the use of the system or device. Quite a few IoT devices that may be used in the healthcare context do not fit well with current organisational

[17] CISCO: The Internet of Things: A CISO and Network Security Perspective, http://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/network-security-perspective.pdf, 2014.
[18] TrapX Security: Anatomy of an Attack. MEDJACK (Medical Device Hijack), https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf, 2015.
[19] Andy Patrizio: Employees circumvent IT security when it slows them down, http://www.itworld.com/article/2711468/security/employees-circumvent-it-security-when-it-slows-them-down.html, 2013.

standards. Particularly with respect to introducing IoT in the organisation's ICT environment, the asset addition rate may often exceed the IT department's capacity to follow appropriate Asset Management and Change Management processes that integrate security checks of new systems/devices.

- From an organisational perspective very important is the behaviour of the users, which is a significant vulnerability specifically in the case of healthcare. The primary goal is patient's safety and physicians will take all the decisions needed on the spot to achieve this goal. Often this means that workaround solutions will be followed. In a smart environment, where a security control is difficult to implement due to the disperse nature of the setting, you cannot afford workaround solutions that can jeopardise the security level achieved. These workarounds often are neither documented nor tested comprehensively and constitute a core vulnerability.
- Due to clinical needs or due to lack of proper configuration management processes, configurations of systems or devices may not be in line with organisational or industry standards. Lack of standard configuration for similar devices across the board results in an ICT environment where there is no common point of reference when it comes to security vulnerabilities as the same devices may be exposed for different reasons making both the discovery of vulnerabilities and the application of corrective measures very difficult throughout the organisation.

The aforementioned vulnerabilities generally comprise technical aspects inherent to the ICT assets. Clearly some vulnerabilities are more pertinent to certain types of ICT assets than others; for instance, vulnerabilities that are related to lack of proper control of security aspects (e.g. unsupported or non-standard system/devices) are more relevant for networked medical devices or mobile devices. Building-related functions such as power and climate regulation or a door lock system can be vulnerable too as they increasingly rely on ICT assets.

## 3.2 Threat analysis

This section discusses potential attack points and threat types based on the key assets and a series of root causes. The root causes of threats faced by smart hospitals are malicious actions, human errors, system and third-party failures and natural phenomena.

The threat taxonomy is focused on cyber security aspects with relevance to Smart hospitals, many of which also generalise to any IT systems. The taxonomy was developed drawing on findings from the interviews and desktop research. Previous ENISA reports have also been employed as a basis for the taxonomy (including ENISA *Threat Landscape and Good Practice Guide for Internet Infrastructure 2015,* and *ENISA Study of IPT and smart grids in 2016*).

### 3.2.1 Threats taxonomy

An illustration providing an overview of the threats faced by smart hospitals is depicted in Figure 6.


**Figure 6 Threats to smart hospitals**

1. **Malicious actions** are deliberate acts by a person or an organisation. Although both threaten smart hospitals, it is important to distinguish malicious actions from other deliberate actions that bypass policies and procedures without malicious intent. A person carrying out a malicious action may be an external or an internal from the perspective of the affected organisation.
   - **Malware** has been identified by the respondents as a major threat for smart hospitals. Malware, which may be more or less directed to specific organisations or types of organisations, is relevant because it allows attacking a large number of organisations with rather low effort. In terms of specific malware concerns, ransomware has been identified as a major threat for healthcare organisations. Other categories of malware include **worms** (which spread between computers), **trojans** (which act covertly), **viruses** (which spread internally), **rootkits** (which hide infection), **exploitkits** (which exploit vulnerabilities in clients to infect

systems), **botnets** (which place many infected systems under control) and spyware (which monitor systems). Malware is a major threat as it can infect a great number of end devices and the multitude and heterogeneity of such devices in a smart hospital (from stationary devices and computers to mobile devices and wearables) result in a particularly large attack surface;

- **Hijacking** may be performed at network level (network/session hijacking – HTTP/TCP) or at device level. The latter is of particular significance in the context of smart hospitals; TrapX Security recently introduced the term "**medjack**" to refer to the hijacking of medical devices to create backdoors in hospital networks[20];
- **Medical device tampering** is another critical threat. Networked medical devices may be reprogrammed, reconfigured by changing device settings or deactivated;
- **Social engineering attacks** (e.g. phishing, baiting) play a particular role in the context of smart hospitals. Social attacks are popular as the human element is usually the weakest link in the defence of an organisation;
- **Device and data theft** are also relevant in the context of malicious attacks; it's a rare attack[21] when considering the volume some of the medical equipment might have. However when introducing sensors, volume is not an issue anymore and the likelihood of this attack to be realised increases. Not having all the interconnected devices in place might lead to wrong data collection, wrong analysis thus wrong decision making.
- **Skimming** is an eavesdropping attack on the high frequency RFID tokens[22]. It's a very specific type of attack however since RFID tags are used widely in the context of smart hospitals (tags, sensors etc) this is very relevant and needs to be taken into account as the protection from this kind of attacks relies more on hardware investment.
- **Denial-of-service attacks** might render a system or service altogether unavailable, which could potentially fully disrupt a patient care process. As smart hospitals tend to rely on web or cloud resources more and more, a DoS attack might, for instance, result in unavailability of patient data (e.g. if data is stored in a cloud environment or if their collection is Internet-based for remote patient care purposes).

2. **Human errors** occur during the configuration or operation of devices or information systems, or the execution of processes. Human errors are often related to inadequate processes or insufficient training. Examples include:
   - **Medical system configuration error** that may compromise either the operation or the cybersecurity posture of the system, or both;
   - Absence of **audit logs** to allow for appropriate control - e.g. of access to smart hospital resources – and/or incident identification and assessment of corrective/improvement actions;
   - **Unauthorised access control** or lack of processes is highly pertinent to smart hospitals particularly due to the sensitivity of patient data involved and due to the fact that the medical processes involve roles with a high level of specialisation in different domains.
   - **Non-compliance**, especially in the Bring Your Own Device (BYOD) paradigm. This is especially pertinent for smart hospitals that rely on mobile applications that can be accessible/installed (e.g. as mobile apps) in personal devices not explicitly approved (and thus tested or adequately hardened) by the hospital's IT department.
   - **Physician and/or patient errors** are a major threat in the context of a smart hospital where there is heavy reliance on ICT assets but the users are not specifically IT experts (e.g. medical staff). Such errors may, for

[20] TrapX Security: Anatomy of an Attack. MEDJACK (Medical Device Hijack), https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf, 2015

[21] http://www.bbc.com/news/uk-wales-22109590

[22] Skimming attack can also be linked to credit card fraud, however in this case it focused on the RFID tokens eavesdropping attack.

instance, be the result of fatigue and poor concentration due to long working hours, or shortcuts or workarounds due to policies and procedures perceived as overly laborious or time consuming (and thus as hindering the patient care process).

3. **System failures** are highly relevant in the healthcare context, particularly due to the increasing complexity and dynamics of the systems. Examples include:
   - **Software failures** that impact or completely disrupt a medical (e.g. failure of a PACS) or administrative process (e.g. patient data availability compromised);
   - **Inadequate firmware**, particularly relevant for the multitude of networked medical devices in a smart hospital;
   - **Device failure** or simply **limited/reduced capability** may severely impact processes that rely, e.g. on the real-time collection of patient data, such as glucose measuring devices;
   - **Network components failure** can cause great impact as the interconnected nature of IoT systems and the need for resilient networking is a core requirement for the functioning of a Smart Hospital;
   - **Insufficient maintenance** which may leave operational issues undetected and unresolved, both in terms of cybersecurity posture, but also in terms of patient care operations;
   - **Overload** can lead to unavailability of a system or service;
   - **Communication between IoT and non-IoT**, particularly as the former grows in numbers, technology and complexity faster than the latter.

4. **Supply chain failure** is outside the direct control of the affected organisation as it typically affects or falls under the responsibility of a third party. As smart hospitals are increasingly dependent on third parties, third-party failures may have far-reaching consequences for them. Examples of third parties a failure of which would have an adverse impact on smart hospital operation include:
   - **Cloud service providers** hosting medical data, applications, systems, administrative data, remote patient data collection points – and other Internet-based smart health applications etc.;
   - **Medical device manufacturer** in cases of failure or non-liability;
   - **Network providers,** such as Internet service providers (ISPs), that support wide area network connectivity and, thus, access to cloud data, remote patients, systems hosted outside the hospital's data centre including national systems (e.g. e-prescription or EHR);
   - **Power suppliers**, a high cross sector dependency that can be partially mitigated.

5. **Natural phenomena** may also be the cause of incidents, particularly due to their disruptive or destructive impact, particularly on the smart hospital healthcare facilities and ICT infrastructure. Moreover, natural phenomena may impact the provision of remote patient care services even if their impact is not targeted to or impacting the hospital itself (e.g. if the metro-level network infrastructure is disrupted due to an earthquake) Examples include:
   - Earthquakes;
   - Flood;
   - Fires.

### 3.2.2 Threat modelling

In this section we provide more information on the type of threat actors that can become potential attackers to a smart hospital and the attack vectors they can affect. Each of these threat actors have different attack surfaces available within Smart hospitals. Threat actors in hospitals include:

- **Insider threats**: These are hospital staff (any role) with malicious intent. This could be physicians, nurses, or even administrative staff that has a malicious intent to harm the ICT systems. These can be potentially the most harmful actors.
- **Malicious patients and guests**: These actors are part of the hospital ecosystem (the patients mostly); they might have a malicious intent which combined with the access they have in the smart hospital assets, can cause great impact.
- **Remote attackers**: In the case of smart hospitals, one of the objective is remote care provision. So use of this equipment for malicious actions could be a possible scenario when the attacker is not physically in the hospital.
- **Other causes**: Environmental or accidental equipment/software failure or even external maintenance staff can cause security incidents, yet have no active attacker.

Attack vectors in hospitals could be:

- **Physical interaction with IT assets**: Physically present attackers (patients or physicians) can directly interact with devices that they have access to. For example: networked medical devices, or interconnected clinical information systems (like a smart pharmacy storing booth).
- **Wireless communication with IT assets**: a very common technique for interception is to attack within range of wireless technologies, including: identification systems or mobile devices.
- **Wired communication with IT assets**: Attackers with wired network communications (including access to the Internet) can interact with related IT assets including cloud services, and online healthcare information systems i.e. drug inventory, patient history. Attackers with physical presence may have direct access to network infrastructure), that they can connect to in order to communicate with other connected smart devices.
- **Interaction with staff**: Social engineering attacks are very common in the healthcare sector, it's usually where ransomware starts from. Instead of targeting the system directly, the attacker focuses on physician/nurse or patient (user with privileged access). Reflected attacks (such as CSRF or reflected XSS) and social engineering attacks can involve fooling or convincing a person to send commands or carry out tasks on their behalf.

### 3.2.3 Asset exposure to cyber threats

In this section the threat exposure of assets is presented.

| CATEGORY | THREAT | ASSETS AFFECTED |
|---|---|---|
| Malicious Action | Virus | Interconnected Clinical Information Systems<br>Mobile Client Devices<br>Data |
| | Ransomware | Interconnected Clinical Information Systems<br>Mobile Client Devices<br>Data |
| | Medical device hijack | Networked Medical Devices<br>Data |
| | Session hijack | Remote Care System<br>Identification Systems<br>Interconnected Clinical Information Systems<br>Mobile Client Devices<br>Networked Medical Devices<br>Data |
| | Device theft | Remote Care Systems<br>Identification Systems<br>Networking Equipment<br>Mobile Client Devices<br>Networked Medical Devices<br>Data |
| | Data theft | Data<br>Interconnected Clinical Information Systems |
| | Medical device tampering | Networked Medical Devices<br>Identification Systems<br>Data |
| | Skimming | Identification Systems<br>Data |
| | Denial of service | Interconnected Clinical Information Systems |
| System Failures | Software failure | Interconnected Clinical Information Systems<br>Remote Care Systems<br>Mobile Client Devices |

| | | |
|---|---|---|
| | | Networked Medical Devices |
| | Inadequate firmware | Remote Care System<br>Identification Systems<br>Networking Equipment<br>Mobile Client Devices<br>Networked Medical Devices |
| | Device failure | Remote Care System<br>Identification Systems<br>Networking Equipment<br>Mobile Client Devices<br>Networked Medical Devices |
| | Network components failure | Networking Equipment<br>Remote Care System<br>Identification Systems<br>Mobile Client Devices |
| | Insufficient maintenance | Networking Equipment<br>Interconnected Clinical Information Systems<br>Buildings |
| | Overload | Networking Equipment |
| | IoT non IoT communication failure | Interconnected Clinical Information Systems<br>Remote Care Systems<br>Mobile Client Devices |
| Human Errors | Medical system conf error | Interconnected Clinical Information Systems<br>Remote Care Systems<br>Networked Medical Devices |
| | Absence of audit log | Networked Medical Devices<br>Networking Equipment<br>Interconnected Clinical Information Systems<br>Remote Care System<br>Identification Systems<br>Mobile Client Devices |
| | Unauthorised access control (misuse of authority) | Data<br>Interconnected Clinical Information Systems<br>Buildings |

| | | |
|---|---|---|
| | Non-compliance with security policies | Data<br>Networked Medical Devices<br>Networking Equipment<br>Interconnected Clinical Information Systems<br>Remote Care System<br>Identification Systems<br>Mobile Client Devices |
| | Physician/ patient (user) error | Data<br>Mobile Client Devices<br>Networked medical devices |
| Supply chain failure | Cloud provider failure | Networked medical devices<br>Interconnected clinical info systems<br>Networking equipment<br>Identification systems<br>Data<br>Mobile client devices<br>Remote care system |
| | Network provider failure | Networked medical devices<br>Interconnected clinical info systems<br>Networking equipment<br>Identification systems<br>Data<br>Mobile client devices<br>Remote care system |
| | Power supplier provider | Networked medical devices<br>Interconnected clinical info systems<br>Networking equipment<br>Identification systems<br>Buildings and facilities<br>Data |
| | Medical device manufacturer failure | Networked medical devices<br>Interconnected clinical info systems |
| Natural Phenomena | Fires<br>Floods<br>Earthquakes | Networked medical devices<br>Interconnected clinical info systems<br>Networking equipment |

| | | |
|---|---|---|
| | | Identification systems<br>Buildings and facilities<br>Data |

### 3.2.4 Likelihood and criticality

The survey participants were asked to rate selected threat categories according to their likelihood of occurrence on a scale from 1 (low likelihood) to 5 (high likelihood). The results indicate that threats based on human errors and malicious actions are perceived to have a particularly high likelihood of occurrence. The likelihood of occurrence for threats based on natural phenomena is perceived as being considerably lower than the ones of the other categories. The full results are depicted in Figure 7.

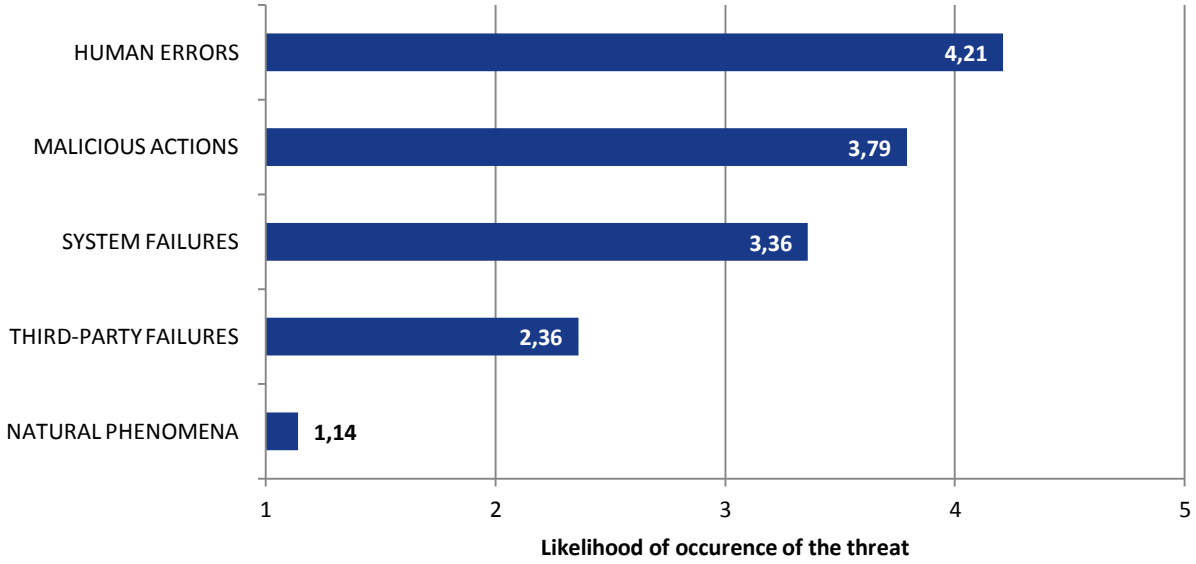


**Figure 7 Likelihood of occurrence of threats**

Additionally, the participants were asked to state which threats they consider to pose most risk to smart hospitals.

The risk posed by malicious actions and human errors was rated critical by approximately three quarters of the respondents. The aggregation of the responses resulted in similar values for the two root causes of threats. With respect to malicious actions, among others, the relevance of threats from malware, social engineering, hacking, denial of service and device tampering was highlighted by respondents. Consequently, they are described in more detail within the scope of the presentation of selected attack scenarios in section 6. With respect to human errors, user errors, non-compliance with policies and procedures and loss of hardware, for instance, were perceived as posing considerable risk to smart hospitals. Loss of hardware and other equipment is often considered to be the consequence of theft. To shed further light on the circumstances of equipment theft, it was also selected as an attack scenario to be further investigated.

Malicious actions and human errors are followed in terms of perceived risk by system failures and third-party failures with some distance. Substantially more respondents underlined the relevance of system failures, though. To regard system failures in more detail, the relevance of software bugs and software misconfiguration was underlined.

Natural phenomena were not perceived as posing considerable risk to smart hospitals by the participants.

Figure 8 depicts what threat categories the respondents considered particularly critical for smart hospitals in the sense that they pose a high risk. Although human errors are perceived to have a higher likelihood of occurrence than malicious actions, malicious actions are considered particularly critical for smart hospitals by a larger group of respondents than human errors. A reason for this may be that malicious actions are perceived as having a higher impact on hospitals than human errors.

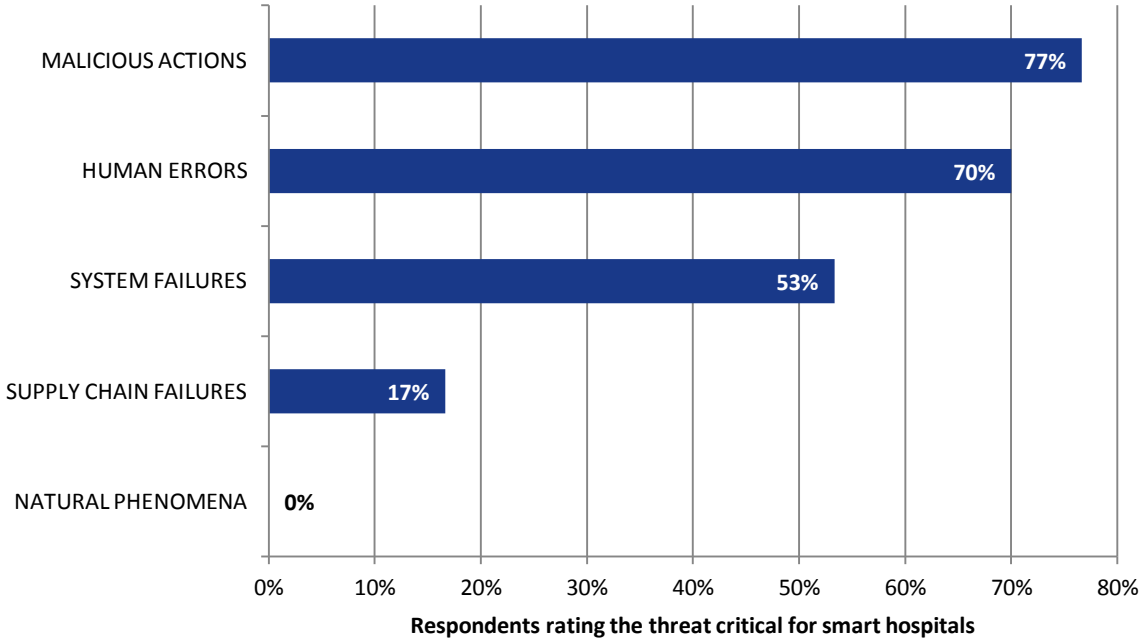


**Figure 8 Threats critical for smart hospitals**

# 4 Attack Scenarios

Five attack scenarios, which are considered particularly relevant for smart hospitals, are described in this section. The respondents were asked to name attack scenarios that they consider common for smart hospitals. Figure 9 depicts the results. In principle, traditional hospitals may also be affected by each of the discussed attack scenarios. For smart hospitals, however, it may not only much more difficult to protect themselves from such attacks but also, should they become victims, the consequences may be much more severe. Protection becomes difficult because, with the high number of networked devices, many potential points of attack are emerging. The consequences become more severe because information systems and devices are more intensely connected within hospitals and across organisational boundaries. Apart from that, the dependence on ICT is generally higher. This section pays particular attention to the aspects that are characteristic of smart hospitals.

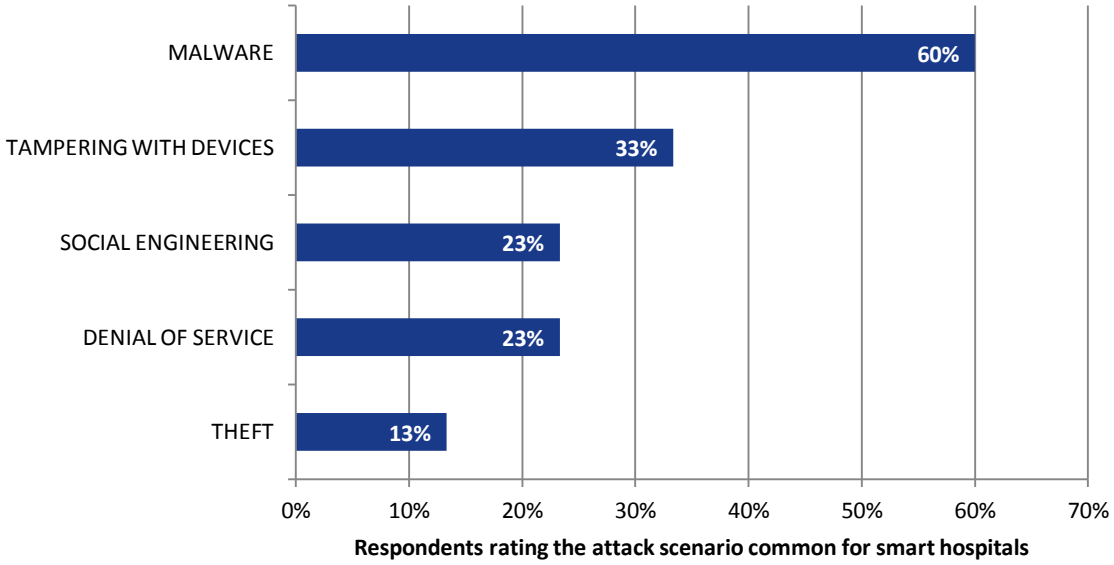


**Figure 9 Attack scenarios common for smart hospitals**

As the concrete examples given in relation to the scenarios show, in practice, the various types of attacks typically do not occur separately from each other. For instance, social engineering attacks are often conducted to better understand the target organisation, which may be a hospital, and to pave the way for follow-up attacks. Attacks that are conducted to better understand the target are also referred to as reconnaissance attacks. It is also possible, however, that social engineering attacks suffice to achieve the objectives of an attacker. Having a good understanding of the target may facilitate not only tampering with or theft of medical devices but also attacks based on the use of malware (e.g. ransomware). As a concrete example shows, even denial-of-service attacks may be combined with other types of attacks such as social engineering.

The main stakeholders affected in the below described scenarios are the patients and the hospital staff; with this including both medical and non-medical staff. In some cases the manufacturers (i.e. of medical devices) are also affected as the equipment they produce is deemed vulnerable to cyber security attacks.

## 4.1 Social Engineering Attack on Hospital Staff

Social engineers typically aim to gather information, commit fraud or get access to systems. Sometimes they conduct attacks to gain insights into a target organisation and to lay the foundation for follow-up attacks, for instance, by installing malware on a computer in the targeted organisation.

| ATTACK SCENARIO 1 | |
|---|---|
| Type of attack | Social engineering attack on hospital staff |
| Description | Social engineering is the human-side of hacking. Attacks can be divided into two categories: human-based social engineering, where sensitive information is gathered by person-to-person interaction exploiting human characteristics such as trust, fear or helpfulness (e.g. pretexting, eavesdropping, shoulder surfing, tailgating, dumpster diving), and computer-based social engineering, which is carried out with the help of computers (e.g. phishing, baiting).<br><br>For a UW Medical hospital in Seattle, a social engineering attack ended with the access of hackers to medical records of 90,000 patients[23]. An employee had opened an e-mail attachment, which contained malware. The malware took control of the computer, which had patient data stored on it. It is not known if the infected e-mail used to attack UW Medical has a spoofed sender address. The likelihood that an e-mail is opened increases if the sender address seems familiar. |
| Assets affected | The assets primarily affected by social engineering attacks on hospital staff include:<br>• Networked medical devices<br>• Networking equipment<br>• Identification components<br>• Client devices<br>• Clinical networked information systems<br>• Enterprise information systems<br>• Data Centre<br>• Information<br>• Staff<br>• Buildings<br><br>Through social engineering, an attacker may get access to hospital ICT assets including networked medical devices, identification components, client devices, clinical networked information systems and enterprise information systems. With respect to non-ICT assets, information and staff are affected. Information can be easily misused with access to ICT assets and social engineering would not be possible without the hospital staff playing its role. |
| Criticality | High – The criticality is high because of the broad range of follow-up attacks that may be possible after a successful social engineering attack. The data breached at the hospital in Seattle, for instance, included sensitive information such as patient name, a medical record number, demographic data including addresses and phone numbers, dates of service, charge amounts for services received at the hospital, the social security number and the data of birth. |
| Likelihood | High – Social engineering has become a pivot point for attacks in the healthcare context. People are considered a particularly weak link in an organisation's security chain. Hospital staff often lacks security awareness. |
| Cascading effects | Social engineering can lead to the compromise of sensitive information, as it happened in the case of the hospital in Seattle by means of a malware attack. Patient data and health records |

[23] Stu Sjouwerman: Social Engineering Causes Seattle Hospital 90K Databreach, https://blog.knowbe4.com/bid/356162/Social-Engineering-Causes-Seattle-Hospital-90K-Databreach.

| ATTACK SCENARIO 1 | |
|---|---|
| | as well as financial information may be the target. Because of the fact that information systems and devices are intensely connected in smart hospitals, a successful social engineering attack may jeopardize a big part of the infrastructure. |
| Recovery time and efforts | It is difficult to make a general statement about the recovery time and efforts after a social engineering attack. Time and efforts depend a lot on the activities of an attacker after a social engineering attack has been successful. Detecting and reacting to an attack quickly is important to keep recovery time and efforts manageable. It is not unlikely, however, that attacks are persistent and remain unnoticed for a long time. At the hospital in Seattle, IT staff discovered the incident on the day after the infected e-mail attachment was opened by the employee. The incident response team immediately took measures to prevent any further malicious activity. |
| Good practices | The key measures to be taken in connection with social engineering attacks on hospital staff include:<br>• Trainings and awareness raising<br>• Policies and procedures<br>• Security organisation<br>• Audits<br>The most important way to protect against social engineering is staff training with frequent refreshers. Awareness for social engineering attacks in particular and information security in general is essential. Additionally, clear policies regarding, for instance, request verification, the use of social media and the reporting of suspicious people or situations may reduce the risk to become victim of a successful social engineering attack. Moreover, clear roles and responsibilities are important to avoid and quickly respond to social engineering attacks. Social engineering penetration tests may be a particularly effective way to create awareness for the threat. |
| Challenges and gaps | Anyone, even security professionals, can become victims of social engineering attacks. As long as there is a conscious interface between humans on the one side and systems and devices on the other side, social engineering will persist. |

Figure 10 illustrates the flow of a typical social engineering attack[24]. Gathering background information about the organisation to be attacked is important. The information does not only facilitate determining the best person to approach but also planning the engagement. Before information can be extracted, a certain level of intimacy needs to be built with the victim.

[24] The illustration is based on previous work by Lailaek (https://lailaek.wordpress.com/2010/12/08/protecting-organizations-from-social-engineering-threats-3/).

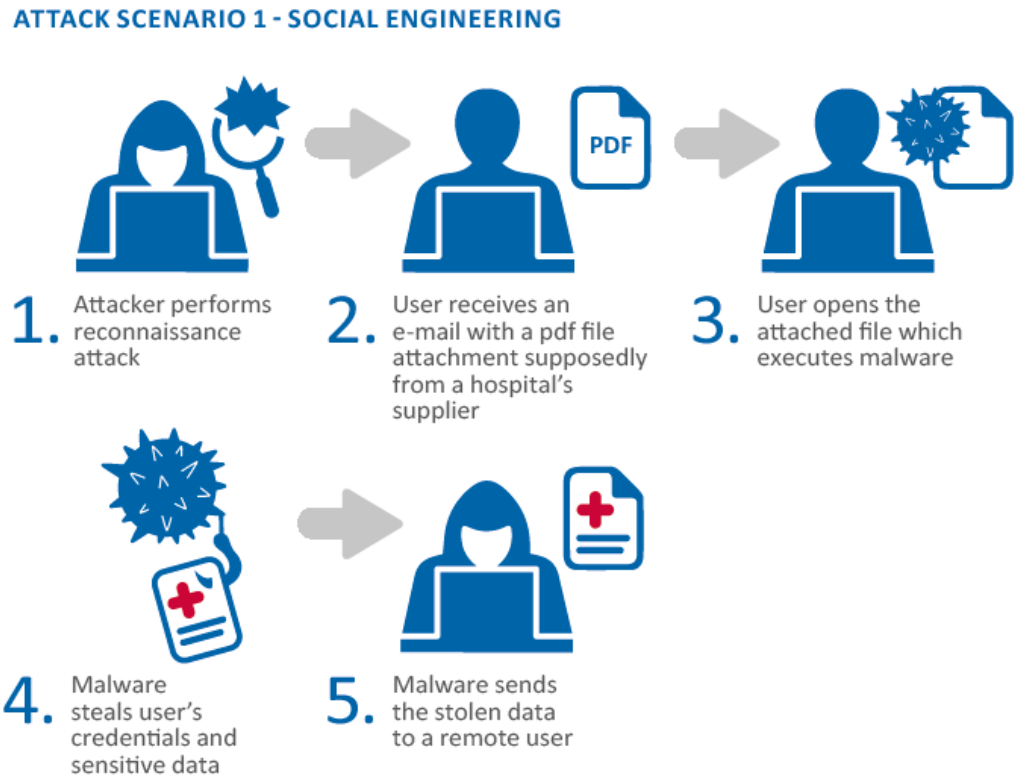


**Figure 10 Social engineering attack on hospital staff**

## 4.2 Tampering with Medical Devices

Compromised medical devices threaten both patient safety and privacy. Moreover, they may lay the foundation for follow-up attacks.

| ATTACK SCENARIO 2 | |
|---|---|
| Type of attack | Tampering with medical devices |
| Description | Tampered medical devices do not only threaten patient safety (e.g. if a pacemaker is deactivated or the settings of an insulin pump are manipulated) but also patient privacy and hospital operations in general, if a device is used as bridgehead to the hospital network. Gaining access to a device is a prerequisite for tampering with it. The attempt to gain illegal access to a device or computer system is usually referred to as hacking. Note: Staff with legitimate access can also tamper with devices but this is not always hacking.<br><br>The information security company TrapX gives in two of its investigative reports[25] concrete examples how medical devices have been used to launch persistent attacks on hospital networks. The names of the attacked hospitals were not released. |
| Assets affected | The assets primarily affected by tampering with medical devices include:<br><br>• Networked medical devices<br>• Identification components<br>• Networking equipment<br>• Client devices<br>• Clinical networked information systems<br>• Enterprise information systems<br>• Information<br><br>All information systems and devices can be affected by tampering, particularly, if they are connected to the Internet. According to TrapX, medical devices that have proven vulnerable range from diagnosis equipment (e.g. CT scanners) to therapeutic equipment (e.g. infusion pumps, surgical machines) and life-supporting equipment (e.g. dialysis machines). While TrapX focuses on persistent attacks launched via tampered medical devices, possible immediate consequences for patient health have also been discussed in detail, for instance, in the context of attacks targeting robot surgeons[26]. Apart from the devices themselves, identification components, networking equipment, client devices, information systems as well as information stored on connected systems and devices may be affected. |
| Criticality | High – The criticality is high because of the broad range of follow-up attacks that may be possible. Medical devices in smart hospitals are increasingly connected with clinical and enterprise information systems. The key problem is that highly vulnerable devices are brought together with highly valuable data. |
| Likelihood | High – Medical devices have become a key pivot point for attacks in the healthcare context[27]. The devices are considered an easy and particularly vulnerable point of entry. |

[25] TrapX Security: Anatomy of an Attack. MEDJACK (Medical Device Hijack), https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf, 2015 and TrapX Security: Anatomy of Attack. MEDJACK.2. Hospitals Under Siege, http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf, 2016.

[26] Lorenzo Franceschi-Bicchierai: Why We Should Be a Little Paranoid About Hackers Messing With Robot Surgeons, Motherboard, http://motherboard.vice.com/read/why-we-should-be-a-little-paranoid-about-hackers-messing-with-robot-surgeons, 2016.

[27] TrapX Security: Anatomy of an Attack. MEDJACK (Medical Device Hijack), https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf, 2015.

| ATTACK SCENARIO 2 | |
|---|---|
| Cascading effects | Hacking is particularly critical in the hospital context as it, if successful, may allow tampering with medical devices. This can have far-reaching consequences for patient safety and privacy, and threaten hospital operations in general. Based on access to medical devices, attackers may breach hospital records over an extended period of time. |
| Recovery time and efforts | Medical devices are often in use seven days per week for 24 hours a day. This leads to delays with respect to security problem resolution. According to TrapX, it is not unlikely that the operation of devices, which were found to be compromised, goes on for days as the risk to patients and hospital operations is considered greater when they are taken offline[28]. Recovery time and efforts depend a lot on the individual circumstances. |
| Good practices | The key measures to be taken in connection with tampering with medical devices include:<br>• Software patching and updating<br>• Baseline security measures<br>• Network segmentation<br>• Network monitoring and intrusion detection<br>• Audit<br>• Organisational processes<br>• Contracts<br>There are no third-party security products that can be installed and operated on standalone medical devices. Updating or patching preinstalled software would be critical but is often not (easily) possible. There are technical reasons for this but also reasons related to the regulatory approval by national authorities and questions related to liability.<br>Consequently, if possible and practical, hospitals should operate medical devices behind the firewall and, an in any case, implement multiple layers of security measures to protect them (i.e. defence in depth). It is advisable to separate critical parts of the network from non-critical parts. For some medical devices that are indispensable but difficult to protect, it may be useful to isolate them in a network that is not connected to the Internet. To be able to identify persistent attacks that have already bypassed primary defences, the hospital SIEM system should be supported by deception technology.<br>It is necessary to determine if existing devices are compromised. Existing devices that do not have necessary protections, even if they are not compromised at the time when they are checked, should be retired. New medical devices should only be procured after reviewing the device and the manufacturer; moreover, vulnerability assessments are essential. The IT staff should be allowed to run stringent security tests when reviewing devices. Manufacturers need to implement state-of-the-art security measures (e.g. code signing, data encryption) and have documented processes to determine if their devices are compromised. In general, it is essential for hospitals to closely cooperate with device manufacturers. |
| Challenges and gaps | Tampering with medical devices constitutes a risk that is difficult to calculate for smart hospitals. Due to limited possibilities with respect to securing devices themselves, hospitals have to rely on measures around the devices as well as on the measures taken by manufacturers in line with the requirements formulated by the competent authorities. Medical devices are sometimes managed by the device manufacturer's technicians only; hospital IT staff may have no possibility to manage the device. Once an attacker has established a backdoor within a medical device, the attack is very hard to detect and remediate. Lateral movement within an internal network is very difficult to detect. Even highly |

[28] TrapX Security: Anatomy of Attack. MEDJACK.2. Hospitals Under Siege, http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf, 2016.

ATTACK SCENARIO 2

secure devices can be compromised if they are connected to an infected or vulnerable device or system. Moreover, there is a high risk of reinfection for remediated medical devices.

Figure 11 illustrates the flow of a typical attack that is based on tampering with medical devices. Internet-connected devices that are vulnerable may be identified using search engines such as Shodan[29]. Apart from the Internet, a weakly protected wireless network may be a way for an attacker to get access to a device. A shellcode execution technique may be used to inject malicious code into a vulnerable device. The attack of other devices and systems can include the lateral movement between network segments.

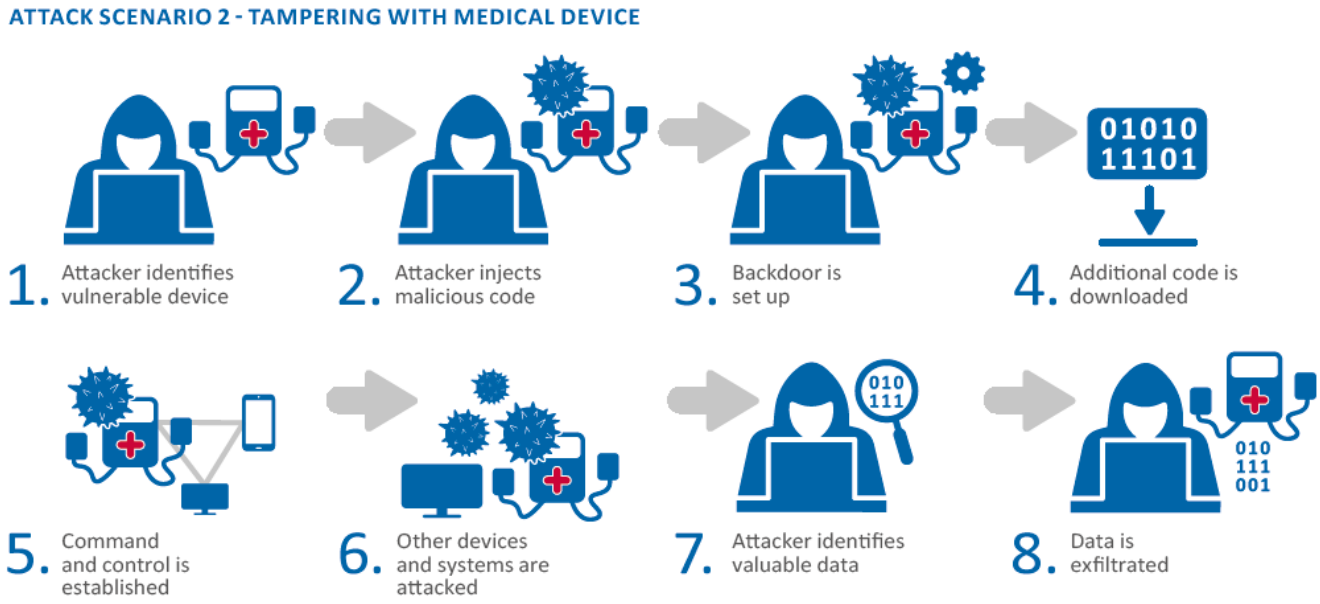


**Figure 11 Tampering with medical devices**

[29] https://www.shodan.io/

## 4.3 Theft of Hospital Equipment

Theft of medical equipment may cause substantial costs for the healthcare sector. Moreover, it may threaten patient privacy.

| ATTACK SCENARIO 3 | |
|---|---|
| Type of attack | Theft of hospital equipment |
| Description | Hospital equipment or hardware theft is the taking of assets without prior permission of the asset owner. The popularity of mobile and wearable devices has led to an increase in the relevance of equipment theft, particularly in the context of smart hospitals.<br><br>In the UK, the North West London Hospitals NHS Trust, for instance, had written off more than £220,000 for a one-year period in 2010-2011 in stolen medical equipment[30]. The NHS North Central London admitted a while ago that an unencrypted laptop containing details of 8 million patients was stolen from a storeroom. Brighton and Sussex University Hospital NHS trusts were fined £375,000 after 232 computer hard drives containing sensitive financial and medical information were stolen from Brighton General Hospital. |
| Assets affected | The assets primarily affected by theft of medical equipment include:<br><br>• Networked medical devices<br>• Identification components<br>• Client devices<br>• Information<br><br>The affected assets are primarily mobile and wearable devices but other equipment such as identification components may also be taken. Sensitive information may be affected in some cases of equipment theft. |
| Criticality | Medium – The criticality is medium. Apart from the material damage suffered though the theft and the risk to patients who depend on medical equipment, sensitive information stored on the hardware may also be at risk. |
| Likelihood | Medium – The likelihood of medical equipment theft is medium. Although all kinds of equipment are stolen, laptops used by hospital staff are the most frequent target of thieves. This makes theft a particularly critical issue for smart hospitals were a lot of processes are digitised. In a smart hospital context, a stolen laptop that is not properly encrypted is more likely to give access to many resources via remote access than in a traditional hospital context. The likelihood is medium as there are different types of equipment to be stolen and sometimes due to size restrictions it's not possible to steal them. |
| Cascading effects | Theft of medical equipment may lead to follow-up attacks. Equipment may be manipulated and brought back into the hospital. Moreover, the fact that the most frequent targets are staff laptops, sensitive information is at risk. |

[30]John Naish: The great hospital robbery: Defibrillators, baby heart monitors, even beds - thieves are walking out of NHS wards with vital equipment, http://www.dailymail.co.uk/health/article-2208065/Thieves-walking-NHS-wards-vital-equipment.html, 2012.

| ATTACK SCENARIO 3 | |
|---|---|
| Recovery time and efforts | Recovery time may be rather long if the stolen equipment is difficult to replace (e.g. usually not on stock, significant need for adaptation). The North-West London Hospitals NHS Trust had to borrow equipment in order to keep performing vital operations[31]. |
| Good practices | The key measures to be taken in connection with theft of medical equipment include:<br>• Asset and configuration management<br>• Policies and procedures<br>• Organisational processes<br>• Physical security<br>• User awareness<br>Theft of medical equipment is generally more dangerous for smart hospitals than it is for ordinary hospitals. Stolen smart hospital laptops do not only tend to store larger amounts of sensitive information (smart devices generate high volumes of data), but also give access to a higher number of remote resources. However, the increasing use of IoT solutions might also help to prevent, detect and investigate cases of equipment theft in the future. Hospital assets can increasingly be tracked and managed remotely, for instance, by using real-time locating systems.<br>Apart from that, encryption, physical access controls, alarm systems, cables to lock equipment as well as clear policies and processes play an important role in trying to avoid theft of medical equipment. |
| Challenges and gaps | Theft is particularly difficult to avoid if hospital staff is involved. Insiders pose a substantial threat to organizations, because they have the knowledge and access to proprietary systems that allow them to bypass security measures through legitimate means. |

Figure 12 illustrates the flow of a typical theft of medical equipment. The basic attack flow for medical equipment theft is quite simple. The concrete flow, however, may vary considerably depending on the specific circumstances, the equipment selected or the involvement of malicious insiders.

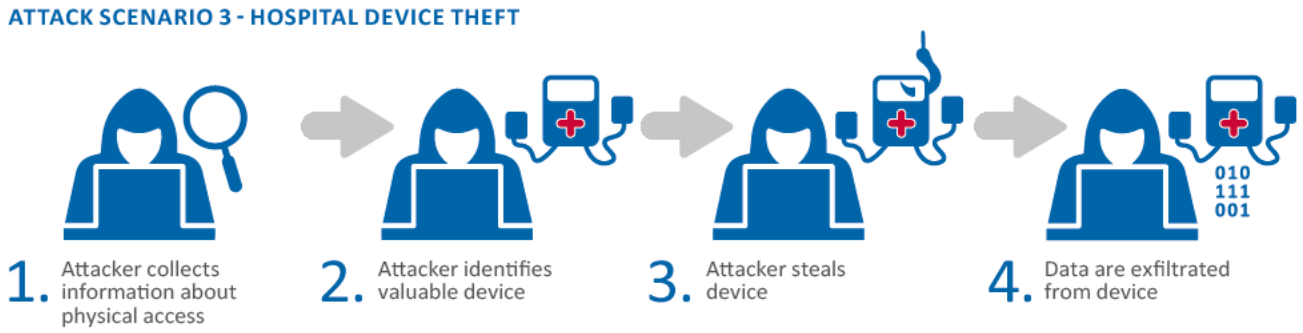


**Figure 12 Theft of medical equipment**

[31]John Naish: The great hospital robbery: Defibrillators, baby heart monitors, even beds - thieves are walking out of NHS wards with vital equipment, http://www.dailymail.co.uk/health/article-2208065/Thieves-walking-NHS-wards-vital-equipment.html, 2012.

## 4.4 Ransomware Attack on Hospital Information Systems

Ransomware attacks prevent the proper operation of their targets. They do not focus on exfiltrating confidential information as tampering with and theft of medical devices typically do.

| ATTACK SCENARIO 4 | |
|---|---|
| Type of attack | Ransomware attack on hospital information systems |
| Description | Recently, hospitals have increasingly become victims of ransomware attacks. Ransomware is a type of malware that restricts access to the infected computer system in some way and demands the user to pay a ransom to remove the restriction[32]. CryptoLocker is a quite well-known ransomware, which has targeted computers running on Microsoft Windows since September 2013. As quite common for ransomware, CryptoLocker was spread via infected e-mail attachments and via an existing botnet.<br><br>At least two hospitals in Germany have come under attack from ransomware. Both the Lukas Hospital in Neuss and the Klinikum Arnsberg hospital were attacked by file encrypting ransomware[33]. It is known that in the Klinikum Arnsberg an e-mail attachment allowed the ransomware to enter the system. |
| Assets affected | The assets primarily affected by ransomware attacks on hospital information systems include:<br><br>• Clinical networked information systems<br>• Enterprise information systems<br>• Information<br><br>Ransomware may restrict the access to the infected information system in various ways. Most ransomware either encrypts the files on the system's hard drive or simply locks the infected system. Accordingly, the affected assets are systems and information. |
| Criticality | High – The criticality is high. A ransomware infection can massively affect the operation of a hospital, meaning the availability of hospital services. While systems can usually be repaired, encrypted data may be lost forever. |
| Likelihood | Medium – The likelihood of become victim of a ransomware attack is medium but increasing. |
| Cascading effects | After the files on the system's hard drive have been encrypted or the infected system has been looked, the actual attack is over. However, as clinical networked information systems as well as enterprise information systems in smart hospitals are connected and as most networked medical devices require access to those systems to function, the impact that ransomware attacks may have on smart hospitals is much larger than the one it would have on ordinary hospitals.<br><br>While the Lukas Hospital's security experts developed special software to cleanse the infected system and scan the 100 servers and approximately 900 devices, hospital operations went on as best they could. Instead of computers, staff had to use pen and paper in the meantime. The fax machine was used to exchange patient's reports. |
| Recovery time and efforts | Time and efforts to recover from a ransomware attack depend a lot on the number of systems affected, whether or not an offline backup is available as well as the respective recovery process times (e.g. time to restore backup, system images/configuration). Detecting and reacting to an attack quickly can help to limit the damage. In the Lukas Hospital, things slowed |

[32] Stefan Lueders and Computer Security Team: Ransomware: When it is too late..., https://home.cern/cern-people/updates/2016/05/ransomware-when-it-too-late, 2016.
[33] DW: Hackers hold German hospital data hostage, http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf, 2016.

| ATTACK SCENARIO 4 | |
|---|---|
| | down considerably, and the staff later had to deal with a backlog of handwritten notes. The ransomware attack affected only data from the time span of a few hours. Nevertheless, the clean-up operation to remove all traces of the malware took weeks. |
| Good practices | The key measures to be taken in connection with ransomware attacks on hospital information systems include:<br>• Organisational processes<br>• Training and awareness raising<br>• Software patching and updating<br>• Network segmentation<br>• Authentication and authorisation<br>Having an offline backup and being able to restore the data from the backup quickly is necessary to avoid having to pay the ransom with uncertain outcome. This requires sophisticated organisational processes. Backups in connected databases are often of limited help as they may also be encrypted. It is critical to detect ransomware quickly and to switch off the infected system as the latter stops the encryption of files. Staff training (incl. regular backup and restore exercises) and awareness raising as well as up-to-date antivirus and anti-spam software are considered key means to avoid being affected by ransomware attacks and to reduce the adverse effects in case of an attack[34]. Separating critical parts of the network from non-critical parts and limiting the privileges of individual users may also reduce the impact a ransomware attack has. |
| Challenges and gaps | Ransomware attacks constitute a calculable and quite well addressable risk for smart hospitals. The key challenge is to select the right measures to be taken as well as to specify a proper incident response plan and ensure its implementation in case of need. It worth mentioning that although, IoT ransomware attacks, can be reversed with a simple device reset, the financial value of locking down IoT ecosystems — and the damage resulting from not unlocking them in time — will rise exponentially. |

Figure 13 illustrates the flow of a typical ransomware attack[35]. The attack flow shows that the spam filter (spam e-mail receives the user), the anti-virus solution (malicious attachment is not removed and binary is downloaded) and the firewall (neither the download of the binary nor the negotiation of the encryption is blocked) must have failed to make such an attack possible. Moreover, the user must have opened the malicious attachment, a Word document, for instance, and enabled the included macro. Before displaying the ransom note, ransomware may not only encrypt the files on the infected system's hard drives but also remove local backups.

[34] Mike Overly: Healthcare Employees at Frontline in Battle Against Ransomware, Healthcare Business & Technology, http://www.healthcarebusinesstech.com/battle-against-ransomware/, 2016.
[35] The illustration is based on previous work by HitmanPro (https://hitmanpro.wordpress.com/2016/02/20/are-you-up-all-night-after-getting-locky/).

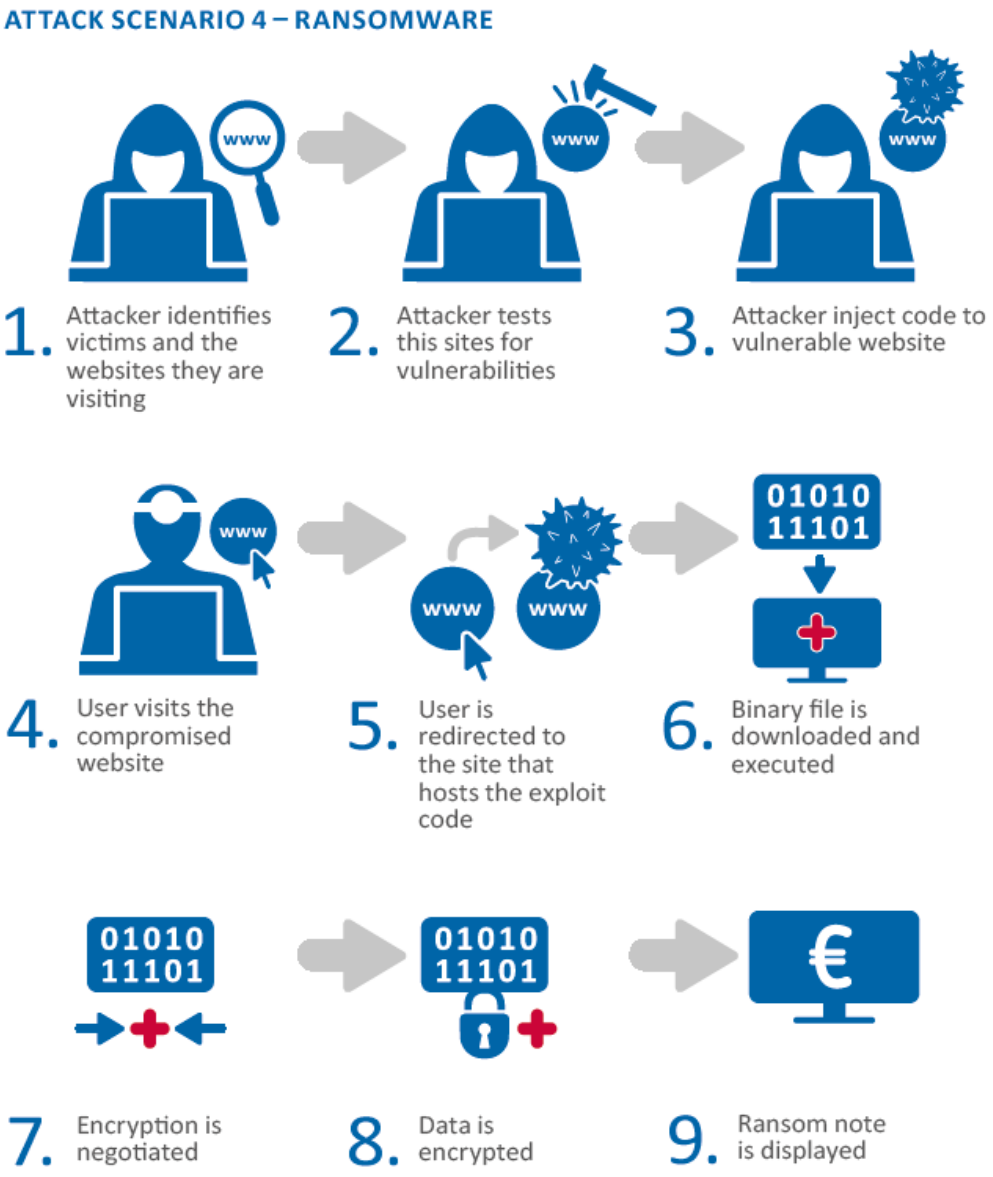


**Figure 13 Ransomware attack on hospital information system**

## 4.5 Distributed Denial-of-Service Attack on Hospital Servers

Just as ransomware attacks, distributed denial-of-service attacks do not focus on exfiltrating confidential information but rather on preventing proper operation.

| ATTACK SCENARIO 5 | |
|---|---|
| Type of attack | Distributed denial-of-service attack on hospital servers |
| Description | Hospitals have become victim of denial-of-service attacks. A denial-of-service attack is an attempt to make an information system or another network resource unavailable to its intended users. An attack is considered *distributed* if there is more than one attack source. A wide array of programmes is used to launch denial-of-service attacks. Distributed denial-of-service (DDoS) attacks are often the result of botnets flooding the targeted network resource with traffic. The largest DDoS attack ever reported was vene carried out via botnet of IoT devices lacking stringent security measures.[36] This shows that it is not only possible that hospitals are affected by DDoS attacks but also that networked medical devices may be hijacked and misused as part of botnets.<br><br>The Boston Children's Hospital (BCH) was victim to a well-documented denial-of-service attack[37]. The hospital was targeted by a hacktivist group. The attack started with a threatening Twitter message that threatened retaliation if the hospital did not take disciplinary action against certain clinicians and return a child to her parents that was taken into custody by Massachusetts protective services before. Over the next days the attack occurred in three major strikes. The first strike targeted the hospital's external website with a relatively slow DDoS attack. The second strike comprised of DDoS attacks as well as non-DDoS attacks. The third strike of the attack peaked at nearly 4-times that of the second strike, reaching 28 Gbps. This time, the attackers also made multiple attempts to penetrate the hospital's network through direct attacks on exposed ports and services. Additionally, the attackers used spear phishing e-mails. These emails tried to lure recipients into clicking embedded links or opening attachments, thereby granting access to a portion of the network behind the hospital's firewall. |
| Assets affected | The assets primarily affected by distributed denial-of-service attacks on hospital servers include:<br><br>• Data centre<br>• Networking equipment<br>• Clinical networked information systems<br>• Enterprise information systems<br>• Networked medical devices<br>• Client devices<br><br>In the first place, hospital servers and networking equipment are affected but unavailability of critical services may keep other information systems and devices from working properly. A hospital may be affected by a denial-of-service attack directly, if a server in the own data centre is affected, or indirectly, if critical third-party services are unavailable due to an attack.<br><br>The BCH incident response team identified three critical potential impacts: inability to route prescriptions electronically to pharmacies, e-mail downtime for departments where e-mail supports critical processes, and inability to access remotely hosted electronic health records. |

[36] Swati Khandelwal: World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices, http://thehackernews.com/2016/09/ddos-attack-iot.html, 2016.

[37] Radware: Anyone is a Target: DoS Attack Case Analysis on Boston Children's Hospital, https://security.radware.com/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/, 2015.

| ATTACK SCENARIO 5 | |
|---|---|
| Criticality | High – The criticality is high. Being victim of a denial-of-service attack can massively affect the operation of a hospital. As smart hospitals are highly dependent on digital records and network connectivity, inability to access systems has potentially far-reaching clinical and business impacts. |
| Likelihood | Low – The likelihood to become victim of a denial-of-service attack is low. Most of the critical systems are not exposed to the Internet, making them less likely to be attacked. |
| Cascading effects | The actual denial-of-service attack is usually limited to making an information system or another network resource unavailable to its intended users. As the case of BCH shows, denial-of-service attacks may be combined with other types of attacks. A DDoS attack can, for instance, be carried out to distract the IT staff while a specific device or system is attacked. |
| Recovery time and efforts | Recovery time and efforts depend on the duration and intensity of the attack as well as the mitigation measures that can be implemented. The BCH incident response team took measures when the second strike of attacks occurred. The measures stopped the attacks from reaching the targeted servers. The first strike, however, had slowed down legitimate inbound and outbound traffic already before. |
| Good practices | The key measures to be taken in connection with distributed denial-of-service attacks on hospital servers include:<br>• Network monitoring and intrusion detection<br>• Organizational processes<br>Network traffic addressed to the attacked network is passed through high-capacity networks with traffic scrubbing filters. Scrubbing filters were also used in the case of BCH. |
| Challenges and gaps | The most serious attacks are DDoS attacks that often involve IP address spoofing so that the location of the attacker cannot easily be identified, nor can filtering be done easily based on the source address. Filtering would require an effort from the Internet service provider when spoofing techniques are used. Moreover, due to outsourced network administration, the hospital IT staff may have only limited possibilities to configure firewalls or routers. |

Figure 14 illustrates the flow of a typical DDoS attack. There are different types of DDoS attacks but all have in common that a network resource is flooded with traffic; messages are sent simultaneously and continuously. The target tries to reply to the requests but after some time gets overpowered and crashes.

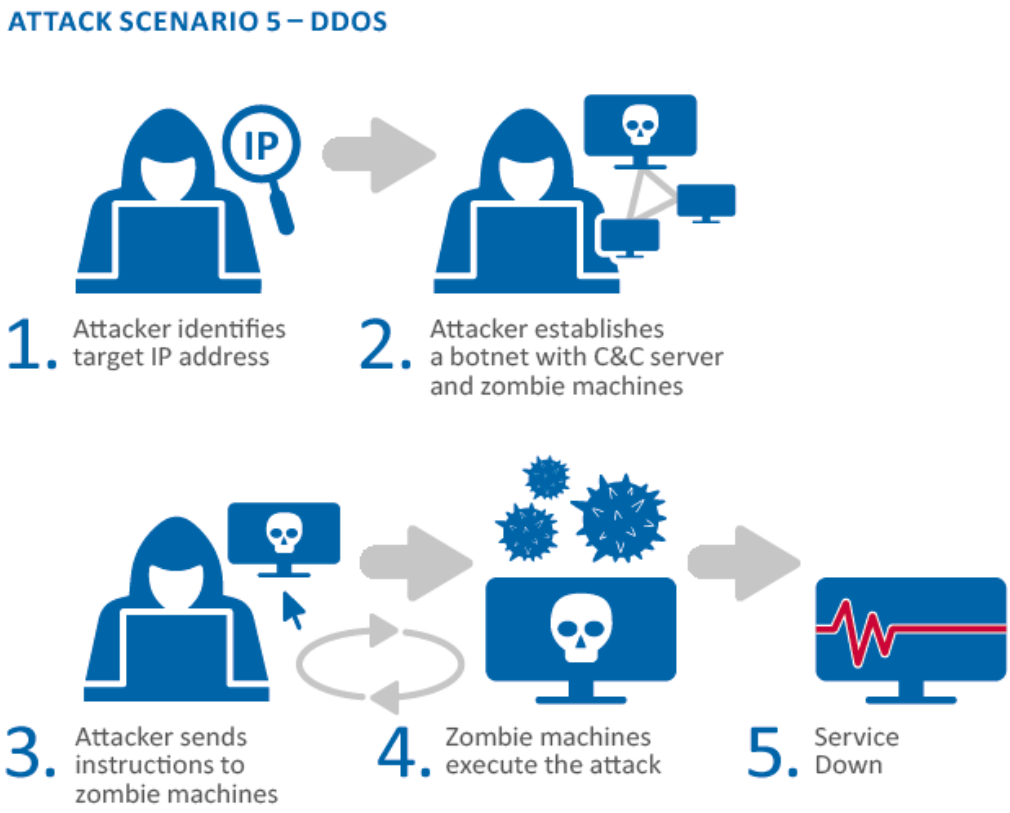


**Figure 14 Distributed denial-of-service attack on hospital servers**

The recruited slave machines constitute a botnet. The purpose of the small-scale attack executed in advance is the discovery of vulnerabilities of the target. Thereby the attacker checks whether the target has taken any precautionary measures.

# 5 Security good practices

The good practices available to protect the smart hospital assets are described in this section. Both smart hospitals and suppliers of smart hospitals need to implement security measures as good practices. Security measures which are also referred to as controls or safeguards are a means of managing security risks and can be classified according to their nature.

- Organisational measures include policies, procedures, administrative tools and methods, and measures to create and maintain awareness[38] and are usually implemented manually. Policies and procedures describe acceptable and unacceptable behaviours of employees in the workplace and function as internal organisational laws[39]. Proactive and reactive means such as asset classification, risk analysis and audits are examples for administrative tools and methods. Although organisational measures may be independent of ICT, they may use information procured by software[40].
- In contrast, technical measures rely on ICT and use software for the purpose of automation. Examples of technical measures are the use of technologies such as firewalls, virtual private networks, intrusion detection and prevention systems and vulnerability scanners as well as the use of cryptography[41].

Figure 15 depicts the responses of the participants when asked for good practices that are not only already widely implemented by hospitals but also considered effective. It is striking that two thirds of the measures considered effective by at least half of the participants are technical measures. Organizational measures, with the exception of a proper security organisation, and regular trainings and awareness raising seem to be considered not particularly effective or not yet widely implemented in hospitals. These are analysed in detail in the coming chapters.

[38] Janne M. Hagen, Eirik Albrechtsen and Jan Hovden: Implementation and effectiveness of organisational information security measures, Information Management & Computer Security, vol. 16, no. 4, pp. 377–397, 2008.
[39] Michal E. Whitman and Herbert J. Mattord: Principles of Information Security (4th ed.), Boston, MA, USA: Course Technology, 2012.
[40] David C. Yang and Liming Guan: The evolution of IT auditing and internal control standards in financial statement audits: The case of the United States, Managerial Auditing Journal, vol. 19, no. 4, pp. 544–555, 2004.
[41] Hein S. Venter and Jan H. P. Eloff: A taxonomy for information security technologies, Computers & Security, vol. 22, no. 4, pp. 299–307, 2003.

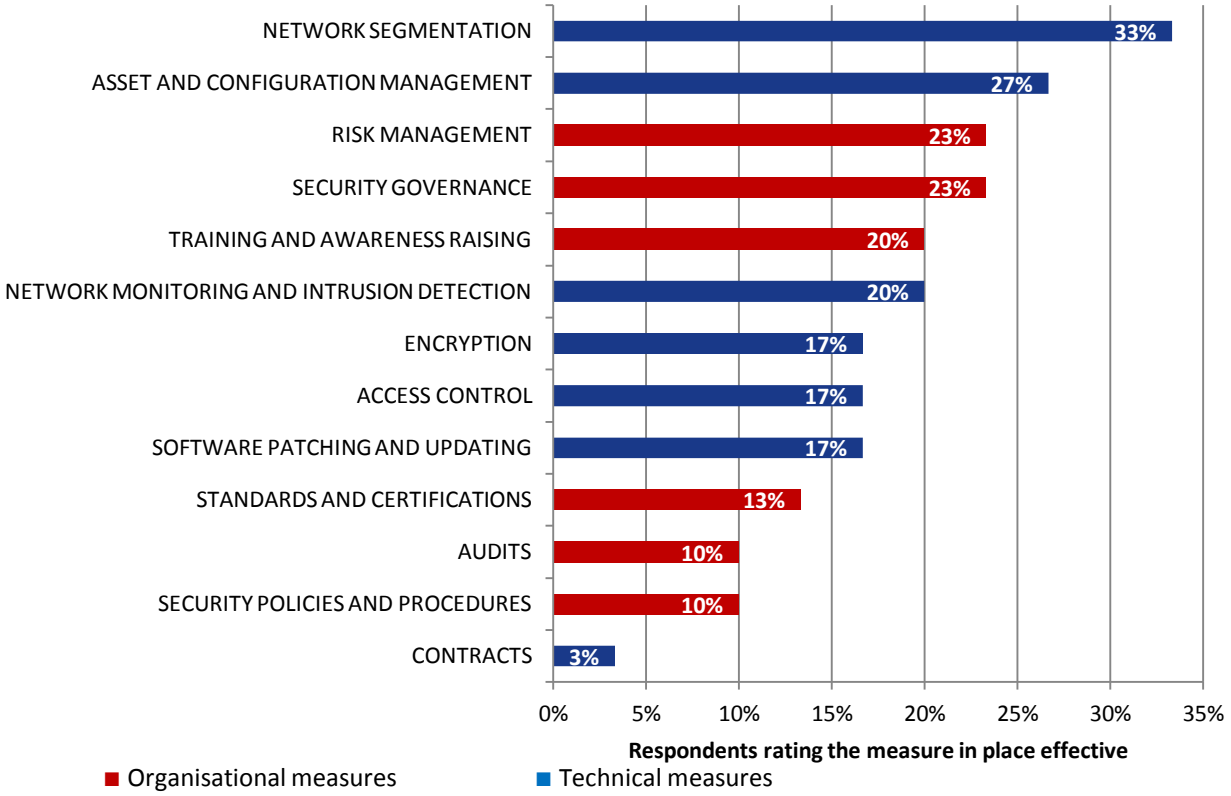


Figure 15 Effective measures in place

## 5.1 Organisational good practices

Most good practices relevant in the context of smart hospitals are also relevant for hospitals. However, as shown below, certain things have to be considered when implementing them in smart hospitals. Moreover, not implementing some of the security measures puts smart hospitals at a greater risk than traditional hospitals.

Organisational measures include, among others, security governance model, security policies and procedures, standards and certifications, training and awareness-raising, risk management, audits and assessments and contractual clauses.

| CATEGORY | GOOD PRACTICE | THREAT GROUP ADDRESSED |
|---|---|---|
| Security governance | **GP 1 – Specify security roles and responsibilities**. Each hospital, especially if IoT components are introduced, needs to meet designated security requirements. A CISO would take the leading role on this activity. In a smart hospital context, particular attention has to be placed on the connection between **security and safety**. Moreover, close cooperation between administrative/clerical staff, clinical staff, the management and IT staff is essential. | Human Errors<br>Malicious Actions |
| | **GP 2 - Create security policies and procedures** which describe the acceptable and unacceptable behaviours of employees in the workplace i.e. security measures regarding mobile devices or other devices that are connected to the medical information systems, the | Human Errors<br>Malicious Actions |

| | | |
|---|---|---|
| | reporting of intrusions and security breaches, the handling of confidential information and the use of personal devices for work-related purposes are example for topics that are particularly relevant for smart hospitals. | |
| | **GP 3 – Develop training and awareness-raising programs**. While awareness-raising activities target rather broad audiences and are intended to make individuals recognise security risks and respond appropriately, training is more formal and has the goal of building knowledge and skills. With respect to training needs in smart hospitals, creating an understanding of the central systems and their components as well as the interactions among systems and components is of particular importance. Even though this has already started emerging, there is still a lot of investment to be done in hospitals using IoT components. | Human Errors<br>Malicious Actions |
| Risk management | **GP 4 – Identify risks, assets and threats** in the smart hospital ecosystem. However, particular attention needs to be placed on the identification of new threats, the detection of changes in vulnerabilities, and the fast and effective handling of incidents. In smart hospitals, which are characterised by a complex and dynamic network of connected devices, the configuration and change management process plays a key role. This process as well as the closely related processes for asset management and procurement need to be properly designed to mitigate risks. Moreover, processes need to be matched with sufficient time and resources to reduce the risk of staff taking shortcuts or workarounds. | Human Errors,<br>Malicious Actions<br>System Failures<br>Supply chain failure |
| | **GP 5 - Develop a contingency plan.** The contingency plan should identify essential hospital functions and associated contingency requirements. It should also address contingency roles, responsibilities, assigned individuals with contact information as well as both information system restoration and implementation of alternative processes when systems are compromised. Examples of actions to be addressed in contingency plans include information system shutdown, fall back to a manual mode, alternate information flows or operating in a mode that is reserved solely for when the system is under attack | Human Errors,<br>Malicious Actions<br>System Failures<br>Supply chain failure<br>Natural Phenomena |
| Compliance and assurance | **GP 6 – Adopt standards** and show compliance through certification. Certifications typically prove that certain products or organisational processes and structures meet certain non-binding minimum standards. In the case of smart hospitals, the components should be compliant to industry standards or to acquire a security certification. | Malicious Actions<br>Human Errors<br>System failures |
| | **GP 7 – Preform often security auditing**. In many cases it is reasonable to ask independent consultants to conduct audits from an outside perspective. Usually audits prove compliance to a standard or a guideline. | Malicious Actions<br>Human Errors<br>System failures |
| | **GP 8 – Perform security assessments**. A self-assessment, a more cost effective measure, can assist the IT staff of the hospital to collect more information on the hospital's information security capabilities and could be based on the internal processes, on suggested good practices or even on public guidelines. | Malicious Actions<br>Human Errors<br>System failures |

| | | |
|---|---|---|
| | **GP 9 – Agree on contractual clauses with manufacturers.** The procurement process for healthcare institutions often starts with physicians asking for very specific devices to be brought in. A tight contract will be overruled by a physician who feels lifesaving therapies are being unduly denied him. Carefully designed contracts play an important role to document mutual expectations both between hospitals and their employees as well as between hospitals and their suppliers. Quite similar to how service contracts specify Service Level Agreements (SLAs), employment contracts or job descriptions can detail the responsibilities of employees in terms of security and safety. Indemnity and warranty protections with suppliers should be transparent. | Supply chain failure<br>Systems failures |

## 5.2 Technical good practices

Technical measures include, among others, asset and configuration management, network monitoring and intrusion detection, patching and updating, network segmentation, and authentication and privilege management.

| CATEGORY | GOOD PRACTICE | THREAT GROUP ADDRESSED |
|---|---|---|
| Cyber security and protection measures (Secure architecture) | **GP 10 – Implement monitoring and intrusion detection/ prevention mechanisms**. Network monitoring and intrusion detection systems are solutions that monitor a network or systems for malicious activity or policy violations. Violations that are detected are typically reported directly to a member of the IT staff or collected in a central database for further analysis, for instance, by means of a Security Information and Event Management (SIEM) solution. External threat intelligence may be used to improve the analysis. Network monitoring and intrusion detection systems may be connected to asset and configuration management systems. Insight into the ICT assets associated with an organisation and access to logs of system events facilitate network monitoring and intrusion detection activities. | Malicious Actions |
| | **GP 11 – Enforce dynamic network segmentation and use of firewalls.** It is important to separate critical parts of the network from non-critical parts. For instance, it is recommended to separate medical devices to the largest possible extent from office components that are typically – due to the use of standard components – susceptible to a wide range of attacks. Moreover, devices with known vulnerabilities that cannot be removed easily may only be used in a separate part of the network or not connected to the network at all. In general, it needs to be evaluated if the benefits of connecting a specific device, such as a magnetic resonance imaging scanner, to the network outweigh the risks. | Malicious actions<br>System failure (avoid cascading effect) |
| | **GP 12 – Run antimalware software.** Computers should run antimalware and anti-spam software (also known as antivirus) to detect and remove or quarantine malicious software. This includes but not limited: medical devices, IT equipment, health information systems, SCADA and Cloud-based data and application services, etc. This can also be a prerequisite for remote care equipment and users mobile devices (in BOYD) to connect to the hospital systems. | Malicious Actions |
| | **GP 13 – Perform regular backups.** This very important action can solve many attacks that could cause great impacts to smart hospitals such as ransomware or physical attacks. Running regular full or incremental backups can be done combined with setting a hot or warm site, making the hospital systems resilient even in the case of natural disaster. | Natural disasters<br>Malicious Action<br>Human Error<br>Supply chain failure |
| Asset security control | **GP 14 – Asset configuration and management.** The complexity and dynamics of the systems of networked devices in smart hospitals makes ICT-based asset inventories essential to ensure a sound understanding of the systems and their components. Such inventories do not only provide an up-to-date overview of the ICT assets associated with a hospital but often also allow changing configurations, and creating and evaluating logs of system events. Some solutions even allow taking advantage of automated remediation (i.e. dynamic policy enforcement). | Malicious actions<br>Human Error<br>System failure |

| | | |
|---|---|---|
| | **GP 15 – Apply patching and updating procedures.** Regular patching and updating of software is essential to avoid the exploitation of known vulnerabilities as well as to ensure the detection of attacks using know paths. Accordingly, in smart hospitals, patches and updates are not only important for networked medical devices and clinical networked information systems, for example, but also for firewalls, antivirus software and other software-based security measures. Ideally, devices and systems support over-the-air manageability | Malicious actions<br>Human Error<br>System failure |
| | **GP 16 - Enforce access control.** Access control is a very important security measure that applies to both ICT and non ICT assets; controlling access to specific devices, assigning specific roles and privileges through separation of duties (in a Smart Room medical staff should be able to make changes to the drug dosage however IT staff should be able to update the firmware). More specifically authentication (ensure identity of an entity) and authorisation (assign privileges) are key security elements. It is essential that authentication is a strong and non-reputable, and that privileges are fine-grained. Usability is an aspect that always has to be kept in mind when dealing with authentication and authorisation. Particularly in hospitals, quick access to systems and devices can be critical. Nevertheless, it proved to be reasonable to grant access to information on need-to-know basis only. | Malicious actions<br>Human Error<br>System failure |
| Data security | **GP 17 – Impose data encryption**. Encryption is one of the most common solutions used in hospitals, mainly because of the criticality and sensitivity of the data at rest, in transit and in use. Health information data stored in third party providers, as well as the ones stored in the hospitals should be encrypted. Encryption standards to be adopted should be based on the classification level of the data. | Malicious actions<br>Human Error<br>Supply chain failure |
| | **GP 18 – Classify Data.** All users, patients, physicians and hospital employees should be granted the least level of privilege/authority necessary to enable them to perform their function. Health data at rest should be classified to ensure that information is only accessible to those that need access. Security personnel should consider the use of access policies that define which users have access to the data, and of enforcement mechanisms that protect at real-time the access of the data from unauthorized read. Access to sensitive data should be under mandatory access control (such as role-based-access-control (RBAC) policies), and should be reviewed and subject to external auditing on a regular basis. Access to data should be logged and logs should be stored in a secure location, to prevent unauthorised alteration. | Malicious actions<br>Human Error<br>Supply chain failure |
| Mobile components security | **GP 19 - Protect Remote and mobile healthcare systems.** Mobile Device Management (MDM) solutions are a particular type of asset and configuration management systems that allow changing configurations and working with logs. They allow better protecting the sensitive data that may be stored on mobile devices. Logs of system events sometimes allow detecting malicious actions or system failures. | Malicious actions<br>Human Error<br>Supply chain failure |

# 6 Recommendations

This section makes concrete and actionable recommendations aimed at hospital executives, industry representatives and policy makers. The recommendations address the national layer (mainly through recommendations for policy makers) and the hospital infrastructure as well as the hospital department layers (mainly via recommendations for hospital executives and industry representatives). With respect to some of the recommendations, good practice examples are formulated. Enabling factors play an important role in the context of recommendations. The survey participants were asked to rate selected enabling factors according to their importance on a scale from 1 (not important) to 5 (highly important). The availability of effective technologies to respond to security threats was considered most important by the survey participants. This fits well with the finding that the major part of the effective security measures in place are technical measures.

Implementing the security measures introduced in section 5 and discussed in the context of concrete attack scenarios in section 6 is necessary but not sufficient to ensure an adequate level of information security in smart hospitals in the long run. This section provides recommendations going beyond the individual measures, which are directed at hospitals executives, industry representatives and policy makers on the EU, the national and the regional level.

## 6.1 Open Issues

The identification of good practices on the topic of cyber security in smart hospitals, let to the identification of open issues; specifically what still needs to be done to enhance cyber security in the vast ecosystem IoT components introduce to healthcare. Below are summarized the most important:

**Gap 1 - Lack of bring your own device controls:** Hospitals should typically prevent patients/employees from connecting their own personal devices to hospital systems (including via Wi-Fi, Ethernet, or VPN), and where this is not appropriate apply effective technical controls to protect the hospital and the network infrastructure from rouge or compromised devices. Due to the lack of control on BYOD mixed infrastructures, these appliances should be kept off the perimeter of relevant servers and services and network access of these devices should be regulated by individual credentials associated to the device (for example, using digital certificates). Wherever possible, these devices should operate under a policy based infrastructure while joining the airport IT domain, giving a more restricted environment (i.e. restriction of peripherals usage via Group Policy).

**Gap 2 - Need of automated asset inventory discovery tool:** Hospitals adopting IoT components need to monitor how these sensors interact with medical devices and systems, and if information collection process is always correct. To achieve this an automated asset inventory discovery tool is needed. This tool enables systems managers to track of all assets and being able to use different discovery methods in case of a disruption. Lack of this makes smart healthcare systems more vulnerable to availability and integrity attacks.

**Gap 3 - Lack of application whitelisting technology (list of authorised software and version):** A very common preventive approach, especially for mobile security, is application whitelisting. This simply means that any application not authorised cannot be installed in the hospital's system. The list can go as far as specifying software version and prevent any entry different than that. In the case of remote healthcare provision this is a major priority as it can be remotely enforced and controlled. Lack of adoption of this technique makes the systems vulnerable as any end user device (remote healthcare provision, wearable medical device, and mobile devices) can be the entry point for an attacker.

**Gap 4 - Need to ensure secure configurations:** hospital information security managers should include cyber security in the requirements when purchasing new equipment when building their smart hospital. Security should be built in

but also (due to the great number of legacy systems) intergratable; patching and updating should be a regular task of information security officers.

**Gap 5 - Need of client certificates to validate and authenticate systems:** Authentication and authorisation is significant in the context of smart hospitals; however due to the disperse nature of its components this is not a priority.

**Gap 6 - Lack of training and awareness-raising programs**. While awareness-raising activities target rather broad audiences and are intended to make individuals recognise security risks and respond appropriately, training is more formal and has the goal of building knowledge and skills. With respect to training needs in smart hospitals, creating an understanding of the central systems and their components as well as the interactions among systems and components is of particular importance.

**Gap 7- Remote administration of servers, workstations, network devices, etc. over secure channels:** Remote services are a benefit of smart hospitals. Introducing this new function in a traditional hospital requires more than a regular monitoring system. The remote devices need to be monitored and sometimes even controlled through a central system over secure channel.

**Gap 8 - Pace of standardisation versus IT technology:** certifications and standards move much too slowly to keep pace with the rate at which lifesaving technology is coming to market. Devices coming to market today couldn't have been dreamed of when some of the standards were just getting started. While these standards are important in many cases, they can inhibit new technologies or fail to account for new failure modes, adversaries, economics, timescales, components, etc.

**Gap 9 – Cost benefit breakdown is critical.** High level executives need to understand the compromise between cyber security measures and impact on services provision. Some expensive controls used in IT security provide some value at high cost, however the trade-off between the impact and the cost is not that big eventually.

## 6.2 Recommendations

### 6.2.1 Hospitals

Recommendations for hospital executives include:

- Establish effective enterprise governance for cyber security: Many organisations, including hospitals, still follow a reactive approach to information security. Measures are frequently taken only after an incident has occurred. In the healthcare context, avoiding incidents is particularly important as trustworthiness is of very high priority. Security incidents may not only threaten personal health information but also patient safety. Nevertheless, hospitals should also be well prepared for the possibility of security incidents by having concrete response and recovery plans in place. More specifically:
  - Perform a cost benefit analysis for the most important IoT components in the hospital. Smart hospital is expensive to implement, it needs to be adequately protected.
  - Create an information security strategy for the smart assets in the hospital. Clear roles and responsibilities as well as regular training and awareness raising activities are key elements of a proactive approach to information security.
  - Create a BYOD and mobile device policy for users; as this is a component of a smart hospital ecosystem this needs to become a priority.
  - Identify the assets and how these will be interconnected (or connected to the Internet). For some systems the right move for safety and resilience might be for the manufacturer to refuse built-in network capabilities into the device.
  - Define and implement security baselines on all major operating systems.

Maps with gaps: 1, 3, 4,6,9

- Implement state-of-the-art security measures: High security typically comes at a high cost and restrictions in collaborating with other healthcare providers and at some point an organisation has to accept the residual security risk. Hospitals must therefore find the right balance for their organisation between protecting and sharing information by setting up security. Hospitals should design, implement and maintain a coherent set of policies, processes and systems to manage risks to their assets. The implementation of state-of-the-art security measures include:
  - network segmentation (smart firewalls)
  - network monitoring and intrusion detection,
  - robust encryption,
  - access control,
  - authentication and authorisation.

Maps with gaps: 1, 2, 3, 4, 7, 9

- Provide specific IT security requirements for IoT components in the hospital: requirements are important for the designers and developers of systems and devices but also for those installing, operating and maintaining the systems and devices at the hospitals. Procurement of security mature products / from vendors with a security track record is a consideration for information security officers in smart hospitals.

Maps with gaps: 5, 7, 8, 9

- Invest on NIS products: currently the NIS market follows a horizontal approach covering all critical sectors. Demand side (hospitals and healthcare organisations) should create the needs for sector specific products that can be customised in any system and can enhance security level throughout the organisation. As the healthcare ecosystem is comprised of many stakeholders, this creates economies of scale which will make these solutions cost effective. Some of these are

- Automated asset inventory discovery tools
- Mobile device management tools
- Security information and event management tools

Maps with gaps: 1, 2, 3, 5,

- Establish an information security sharing mechanism: Hospitals will be the next major target for cyber security incidents, just because the lack of protection mechanism is becoming evident. Smart hospitals that depend even more on ICT will be the step after that. The need to create a community between Hospitals to share information is a very efficient protective measure. Coordinated disclosure policies are becoming a trend. Responsible disclosure about new threats, devices and equipment vulnerabilities, new patched, solutions and mitigation measures can and should involve not only the demand side but also manufacturers and vendors aka the supply side. This approach should be adopted by healthcare organisation actors: physician and patients.

Maps with gaps: 3, 6, 8

- Conduct risk assessment and vulnerability assessment: Security must be comprehensive, otherwise attackers will simply exploit the weakest link. Consequently, vulnerabilities need to be identified and efforts can then be focused on these particular areas. As a comprehensive redesign of the infrastructure with information security in mind will not be realistic in most cases, iterative improvements across all relevant areas, taking into account organisational as well as technical measures, are usually most effective. Hospitals also need to possess the right skills to install, operate and maintain information systems and devices properly. A coherent strategy is critical for improving the interoperability between systems and devices and, at the same time, eliminate potential weaknesses.

Maps with gaps: 4, 5, 7

- Perform pen testing and auditing: Independent security experts help understanding required budgets, staff and key activities to reach a level of information security that is optimal for a specific organisation. An option may also be to involve a managed security service provider to improve security capabilities quickly. External experts may also perform security audits or review compliance with applicable laws and regulations. In the healthcare context, compliance is of particular importance. It may also be worthwhile for hospitals to stay in touch with technology and consulting companies focused on information security. Such companies typically have a sound understanding of the security status, good practices as well as common strengths and weaknesses in information security management across the sector.

Maps with gaps: 4, 5, 7

- Support multi-stakeholder communication platforms (ISACs) and information sharing alternatives: Sharing and discussing good practices and security intelligence among stakeholders is critical to improving the overall security status in healthcare in the EU. A key objective must be to make stakeholders aware of potential threats as early as possible and to facilitate a cross-national approach to finding adequate solutions. Apart from healthcare institutions, manufacturers and governments should be involved in the communication. It does not seem to be necessary to establish any new platforms to support multi-stakeholder communication in the context of information security in healthcare. Existing platforms can well be used on the EU, the national and the regional level. On the EU level, ENISA could intensify its efforts to facilitate the communication among the relevant stakeholders.

Maps with gaps: 2, 3, 4, 5

### 6.2.2 Industry

This report focuses on supporting hospital management and information security experts in investing correctly and cost effectively in protecting smart assets. In order to do so, collaboration with the industry is Recommendations for industry representatives with a clear focus on manufacturers of systems and devices used in smart hospital contexts include:

- Incorporate security into existing quality assurance systems: Taking security seriously and addressing security during product design and development are essential for manufacturers of critical systems and devices, particularly if they are applied in the healthcare context.
  - Following the "security by design" paradigm, which means that a product is designed to be secure from scratch, and the "secure development" paradigm, which focuses mostly on the adoption of secure coding good practices, or implementing the "privacy by default" concept, which requires that the default settings of a product must protect the privacy of individuals, is advisable.
  - Specific guidelines to secure development have been released by various organisations already years ago.
  - To effectively incorporate security into existing quality assurance systems, training and concrete guidelines are essential.
  - Making devices patchable is one of the most effective steps for eliminating vulnerabilities (and cybersecurity risk) in the healthcare environment.
  - Include secure coding practices should be ensured.

Maps with gaps: 4, 5

- Involve third parties in testing activities: Testing is a key element of qualitative product development. To make sure that security-related requirements from users as well as regulators are met, it is important to involve them into test design and execution at an early stage. In the healthcare context, hospitals should play a key role in the testing activities. For instance, cross-testing could be performed in a larger number of hospitals before products are released. Moreover, regular penetration testing and mock by through security companies are advisable to assess security levels. Mock attacks could also be useful for hospitals as they allow determining response times.

Maps with gaps: 5, 9

- Consider applying medical device regulation to critical infrastructure components: The Medical Devices Directive defines clearly what constitutes a medical device. While software used for medical purposes is explicitly included, critical components of the information and communication infrastructure do usually not fall under the regulation of the MDD. Due to their essential and growing role in providing healthcare, an extension of the definition of medical devices might be worth considering.

Maps with gaps: 5, 7

- Support the adaptation of information security standards to healthcare: Currently, there is a lack of standards that meet the specific information security needs of the healthcare sector. This is true for both information security management practices and critical information systems and devices used in the healthcare context. Concrete actions are necessary with respect to standards for products used in hospitals, at EU level and at national level. The EU needs to set standards which are supported by the Member States to ensure that smart hospitals are well-positioned in terms of information security. To achieve this objective, an overview over the processes and policies adopted by hospitals in the various EU Member States is critical. Eventually, certification of hospitals in the EU with respect to these standards through independent experts should be required.

Maps with gaps: 8


## ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

## Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece


TP-05-16-016-EN-N


PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu



ISBN: 978-92-9204-181-6
DOI: 10.2824/28801