

ABSTRACT

<input type="checkbox"/>	Bachelor's thesis
<input checked="" type="checkbox"/>	Master's thesis
<input type="checkbox"/>	Licentiate's thesis
<input type="checkbox"/>	Doctor's thesis

Subject		Date	02.04.2019
Author(s)	Valentin Constantin Ogner	Student number	518506
		Number of pages	59
Title	Is my medical software allowed to go to market?		
Supervisor(s)	Prof. dr. Anne Francoise Rutkowski		
<p>Abstract</p> <p>The central importance of software in healthcare practices is highlighted by the increasing regulation of medical software in order to safeguard medical activities and patient's rights. Medical software suppliers need to meet regulatory requirements from different countries to gain market access and offer necessary compliant solutions. The present report focuses on providing methods and tools to allow software suppliers to evaluate which software products should be sold in which countries. Using design science and behavioral science two artifacts are presented integrating influence of regulatory requirements on market access and product lifecycle management. It is required to present all the regulatory information in an actionable way in order for it to be operationalized by businesses and engineering staff within a company.</p>			
Key words	Software, Medical Device Regulation, Regulatory, Risk Management, Privacy and Security, Quality Management, Market Access, Business Modeling, Product Lifecycle Management, Business Architecture, Healthcare Informatics		
Further information			



**UNIVERSITY
OF TURKU**

Turku School of
Economics

IS MY MEDICAL SOFTWARE ALLOWED TO GO TO MARKET?

Master's Thesis
in International Business

Author (s):
Valentin Constantin Ogner

Supervisors:
Prof. Dr. Anne Francoise Rutkowski
Prof. Dr. Hannu Salmela
Prof. Dr. Patrick Rousseau

1.06.2019
Tilburg

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Table of contents

1	INTRODUCTION	7
1.1	Problem description	7
1.2	Literature	7
1.3	Managing software impact	10
1.3.1	Control software & safety-critical software.....	10
1.3.2	Volume and economy of scale.....	12
1.4	Case considerations malfunctions of safety-critical software	13
1.4.1	CASE 1: Boeing 737 MAX flight control software malfunction	14
1.4.2	CASE 2: Medtronic chamber pacemakers recall.....	14
1.4.3	CASE 3: Philips Cleveland FDA investigation	15
1.4.4	Impact - FDA Volume recall analysis for software.....	18
1.5	Philips VitalHealth company profile and products	20
1.5.1	ENGAGE - Patient and clinician engagement.....	22
1.5.2	COORDINATE - Care coordination and care management	24
1.5.3	QUESTLINK - Outcomes management	25
1.5.4	INSIGHT - population healthcare analytics	26
1.6	Regulation requirements – European union regulatory environment	27
1.6.1	European union medical device regulation (EU MDR).....	28
1.6.2	Product and QMS Certifications for Philips VitalHealth	31
1.6.3	EU MDR Lifecycle approach	32
1.6.4	General data protection regulation (GDPR)	32
1.6.5	European Interoperability Framework (EIF).....	33
1.7	Risk management & control for software in healthcare.....	34
2	METHODOLOGY	36
3	DESIGN SCIENCE	39
3.1	Artifacts, research process steps	39
3.2	Design an artifact: creation of an innovative, purposeful artifact.....	40
3.3	Problem relevance: description of problem domain	48
3.4	Design evaluation: evaluation of the artifact	51
3.5	Research contributions: novelty, innovative problem solving.....	52
3.6	Research rigor: preparations for the build – evaluate loop	53
3.7	Design as a search process: effectiveness of the design - Iterations	54
3.8	Communication of research: technical but also managerial audiences.....	55
4	CONCLUSIONS	56

5	LIMITATIONS & FUTURE RESEARCH	57
6	BIBLIOGRAPHY	58

List of figures

Figure 1 : Medtronic press release - pacemaker recall 2019.....	15
Figure 2 : FDA Investigation report for Philips Cleveland.....	17
Figure 3 : Philips Cleveland FDA recall - software design cause.....	18
Figure 4 : FDA class distribution of software recalls	20
Figure 5 : VitalHealth platform.....	21
Figure 6 : Philips VitalHealth products.....	22
Figure 7 : Population health management portal	23
Figure 8 : Patient portal.....	23
Figure 9 : Care coordination portal	24
Figure 10 : Population health management view	25
Figure 11 : TÜV SÜD– EU MDR Milestones for Philips VitalHealth	28
Figure 12 : Harmonized Standard EN ISO 13485 - QMS requirements.....	31
Figure 13 : Lifecycle approach - BSI Whitepaper	32
Figure 14: European interoperability framework concept	33
Figure 15 : Risk control matrix for healthcare software	35
Figure 16: Strategic alignment: Leveraging information technology	37
Figure 17 : Phillips Q&R compliance requirements for software.....	43
Figure 18: Philips Non-Q&R compliance requirements.....	44

Figure 19 : IS research framework.....	48
Figure 20 : Global compliance heat map of harmonized standards - Belgium.....	50
Figure 21 : Design science evaluation methods table	51
Figure 22 : Australian regulatory roadmap for medical devices.....	54
Figure 23 : Build evaluate loop.....	54

List of tables

Table 1 : Classification EU MDR	30
Table 2 : Dashboard product lifecycle management – general product info	40
Table 3 : Product lifecycle essential requirements checklist	41
Table 4 : Representation of standards for Australia for VitalHealth - part 1	45
Table 5 : Representation of standards for Australia for VitalHealth - part 2.....	46
Table 6 : Essential requirements checklist.....	47
Table 7 : Regulations harmonized standards table for Australia	49
Table 8 : Product - global approbation matrix - market access	52
Table 9 : Approval status legend.....	53

1 INTRODUCTION

1.1 Problem description

The increased importance of software in healthcare justifies stricter regulatory oversight by governments, mainly safeguarding patient's rights and establishing the essential principles and limitations in which software in healthcare operates.

International medical software suppliers need to meet regulatory requirements from different countries to gain market access and offer compliant solutions. There is a shortage of methods and tools available to allow software suppliers to evaluate which software products to sell in which countries. In order to bridge the gap in method approach and tool availability, the research conducted in this report focuses on three main questions.

- How to stay in compliance with regulatory requirements and export controls during the product lifecycle for medical software?
- How to present the regulatory regional information during the product lifecycle to the various stakeholders?
- How to organize the business to ensure delivery of value-added solutions with timely market access?

By following these questions, the aim of the research is to offer the groundwork for a healthy practice on how to bring medical software products to the market while paying attention to all the relevant stakeholders involved.

1.2 Literature

Technology plays a significant role in the management of healthcare services. Healthcare informatics and Enterprise Resource Planning (ERP) systems claim to support the evolution in healthcare services by interconnecting data and records, providing a firm foundation for quality improvement in healthcare services and outcomes (Kolodner, 2008).

Software companies started considering development scenarios, at the intersection of medical informatics, public health, and business. The information delivered through communications systems enhances the healthcare practice by adding the complexity needed for the medical act (Eysenbach, 2001).

According to the research, performed by Radley(2013) the reason to push for healthcare informatics and eHealthcare is to reduce the risk of making medication errors

and to provide appropriate care paths for patients. Considering the nature of information and procedures involved in patient monitoring, diagnosis and treatment healthcare software are classified as a safety-critical software. One wrong recommendation, medication flaw, or treatment error can put the patient's life at risk. The demand for clinical decision support systems increases and software companies want to serve this market by offering relevant compliant solutions. Healthcare information systems and coordination of healthcare professionals through Information & Technology (IT) provide the interdisciplinary cross-department exchange of information improving clinical decision quality (Middleton, 2016) and consumer satisfaction (Eysenbach, 2001).

The essential requirements checklist for eHealthcare software development and implementation must contain clear practices defining the following aspects:

- Security
- Privacy
- Regulatory
- Required Language
- Support
- Hosting
- Software
- Hardware
- Labeling - instructions of use
- Technical documentation
- Medical definitions
- Risk profile

Healthcare organizations are struggling with developmental issues when addressing healthcare informatics and ERP implementation. Information Systems (IS) implementation in Healthcare need continuous improvement on confidentiality, integrity, privacy, and patient trust. Ensuring end-to-end security and privacy procedures in healthcare informatics is a mandatory consideration. Security and privacy should be internal at every level in the process. This, by starting from the point of data collection through various sensor and mesh-networks, integration of internet of things, and continuing with the infrastructure communication links, data storage, access management, and enterprise governance (Sahi et al., 2017).

Security and privacy are important aspects of the essential requirements checklist and regard healthcare organizations end-to-end. The consequence of this consideration is that security and privacy by design become a mandatory practice in the process of creating medical software.

Hospitals gain extensive amounts of information and data from several assets and departments. An integrated system, such as an ERP system, allows health organizations to improve service efficiency and the quality of care by better managing information coming

from various services and processes (Handayani et al. 2013). Electronic healthcare records, as well as healthcare process data, represent high-value information according to the data subject. From the patient perspective the security and privacy issue become an important aspect (Sahi et al., 2017).

Most research in healthcare informatics addresses the implementation of information systems, care coordination, and patient/doctor platforms. The research includes information systems security and risk management (ISSRM) practices that safeguard sensitive data and assets in healthcare (Mucheleka, 2015).

Addressing security and privacy concerns for healthcare organizations requires combined ISSRM with hospital enterprise architecture (EA) framework principles. The framework principles are access control, authentication, non-repudiation, and accountability, segregation of duties, gate control without which end-to-end security and privacy cannot be ensured (Sahi et al., 2017).

General-purpose healthcare informatics mostly is handled by generic health ERP systems. However, it is advisable to use service-oriented architecture (SOA) applications. SOA applications are not part of the standard implementation of ERP. SOA applications are developed for more specific purposes in healthcare. The EA literature enforces the development of microservices and applications using SOA because this is highly beneficial to the system development process (Joyce, 2017). To ensure the end-to-end integrity and coherence around sensitive patient data, by adding software applications to the overall ERP healthcare information system, ISSRM frameworks also need to be aligned for the SOA developed applications (Mayer, 2018).

End-to-end implementation of healthcare ERP systems have by design ISSRM frameworks built in. Because of the specificity of certain healthcare activities, microservices and applications have to be implemented through SOA into the overall EA of healthcare information systems. Furthermore, solutions have already been considered for the design of applications, that run on mobile devices and help doctors display images and information about health records. These solutions can be managed through a multi-layered SOA. It is essential to organize healthcare information assets in order to achieve the greatest efficiency and effectivity of resources available to healthcare organizations through SOA. Sahi et al. (2017) and Midha (2017) state that healthcare information systems and ERP systems are unable to answer some of the sensitive questions, regarding personal healthcare data. Sahi et al. (2017) and Midha's (2017) reports also underline the relationship between two aspects: confidentiality and user trust. Privacy regulation ensures confidentiality of patient's data. It accelerates the adoption of healthcare informatics and eHealthcare solutions, increasing the level of trust from patients

The software manufacturers claim to be aware of applicable legislation and information security requirements. Such that it takes all necessary actions to achieve and con-

tinuously enhance compliance with state-of-the-art standards. Risk management structurally identifies and analyzes potential information security breaches and manages the required preventive and corrective measures. Software development is documented in all stages of design and development. The technical files are concrete evidence of work practices and the quality of the product and serve the scrutiny of internal and external audits to claim compliance with a specific standard. Harmonized standard practices can be adhered to build a trustworthy relationship with the healthcare organization and medical software provider.

1.3 Managing software impact

In society, software impact can be measured based on the how critical are the activities it serves and how big is the installation and deployment scale. Clinical decision is a critical aspect in healthcare organizations. Decision control becoming part of automated software design instead of manual control, therefore pushing for risky decisions to be managed by software. Therefore, the need for safety-critical software. The volume in which software is installed defines the deployment scale. When software has a wider install base it becomes more relevant to society. The volume of sales given also judges economic success by the fact that the cost of software reproduction and distribution is zero.

1.3.1 Control software & safety-critical software

The importance of software in society is increasing rapidly. Moreover, control and critical decisions are entrusted to software systems. According to the research performed by (Rutkowski, 2017). the growth of software systems is typically around 20% per year. The growth of safety of control related software systems however is only 10%, even though the importance of software in society is increasing. This discrepancy is increasing (rep) while trying to close the gap between demand and supply for control related systems with software solutions that are not dealing with critical risks and lacking defensive coding techniques. Instead, the control remains with software systems on critical aspects, leading to unwanted risks and dangers in society.

A clear distinction between typical software and control software can be observed in development and implementation. Safety-critical elements in control software are in detail acknowledged in the design phase. Error, failure scenarios should be well documented and known. The design and code are tested extensively so failure scenarios are avoided at all cost. Safety-critical engineering is a good practice in software development when dealing with control software.

Medical software can harm patients and should therefore be treated in a similar way for example as flight management systems. The risk category can be considered similar to software developed for navigating air flight shuttles, flight management systems, and train traffic control by measuring the impact on healthcare informatics. Because of the risks involved in healthcare informatics on patient harm, the same type of defensive coding practices is used to protect the systems from unpredictable errors that can put patients' lives at risk. Constructing defensive coding involves exponential growth of lines of code (LOC) in comparison with the typical coding of software.

Over the past 40 years, the amount of code used for flight and land procedures for spacecraft's on Mars has grown exponentially. The improvement in defensive coding practices and new coding standards in air flight control software:

- 1975: the Viking landers had about 5 KLOC onboard,
- 1998 Pathfinder had 150 KLOC,
- 2003 the Phoenix lander had 300 KLOC,
- 2004 the Mars exploration rovers each had 650 KLOC
- 2012 the Mars Science Laboratory (MSL) Rover had 3 MLOC.

At first glance, the connection between landing a spacecraft on Mars and how Healthcare Informatics works is not evident. Preventing, detecting, and containing are the three main control process principles in the creation of control software. However, most software development projects use coding standards for a different approach. In usual software development, some of the coding standard are ignored to increase the time to market, issues mitigated by the deployment of patches. As is often the situation with other coding standards. Regulations and standards cannot be quietly ignored when considering defensive coding and safety-critical software. Apart from the coding skills, software developers need to understand how air flight operates in real life. Software risk-defensive programming skills become mandatory in control software (Holzmann, 2013).

Having risks mitigated in the prevention phase proves to be a successful strategy with fewer risks to manage in the later stages. Risk profile tables are used to store the identified risk behaviors based of the usability scenarios for the software product. Based on the risk profile, it is mandatory to mitigate the main critical risks in the design phase. After the mitigation of the main risks, residual risks remain unaddressed. The residual risks are also addressed by mandatory mitigation actions, until the risk benefit ratio gives a green light.

In the detection phase, the risks and vulnerabilities present in the code must be identified as early as possible in the development cycle. The code is as good as the testing and code review. As an example, in the air flight control software for the Rover landing on Mars, 80% of peer review and comments were accepted and reviewed (Hevner, 2004). All the accepted peer reviews and comments had an immediate action assigned to them. For a single instance of the module of the software flight control, 10,000 peer comments for the process were produced with 25,000 tool reports in the detection phase.

The code was tested; Routine checks were conducted for common types of coding errors. Compliance issues with the coding standard or risky code patterns were identified.

Defensive coding makes also testing very difficult because it prepares the system to react to unpredictable errors:

- ensuring the reliability of the last instance of any large and complex software application
- building defensive actions enforce containment around the residual risk, containing it not to spread to other modules
- building redundancy in the software
- limiting software subsystems to critical action modules
- giving the second chance to control a critical switch with code that is different from the one used in the previous instance

There are no notable problems reported in air flight control caused by software problems, therefore defensive coding principles prove to be the solution when dealing with critical control and safety issues.

1.3.2 Volume and economy of scale

If impact can be measured by the critical/risk profile it operates in, the impact of software can be measured by the amount and volume of software deployed around the world. Hence, the more the spread the higher the relevance for society. If the relevance for control software for airspace maybe very specific, error-proof and safe, only some submodules of the software systems can be reused for future airspace control systems. When considering reusing systems for different scenario, the chance to scale-up is limited. Mostly, because every air flight routine is different to the previous one. To deploy the same air flight control software, it has no relevance beyond the initial scenario build.

The software's affordability stimulates its relevance, the smaller the installation base, the higher the development cost per usage. The installation base must therefore be increased to make the software affordable. The result is that software as a business becomes more profitable. Economically, it makes sense to increase its volume deployment as software replication costs are close to zero. Increasing the installation base is can also be prerequisite of innovation. Although the software may well be technically clever and functional, it simply cannot work economically without amplifying the volume for software especially for its subsequent maintenance.

However, amplifying the volume of software requires a different approach concerning the risk profile compared to critical safety software systems. This risk is even growing when enlarging the install base. Usually, a software bug comes with multiple not when considering volumes. If the error happens for one user, it is likely to happen for more

users. Let us consider this scenario, if a software has a user base of 100,000 subscribers and a probability of a software bug appearing of 5%, for sure 5,000 of those users will get the software error. In addition, if that error is critical and generates collateral damage and harm, liability will arise. These liabilities have an immediate effect on the business side. In the next subchapter, three cases of liability outcomes are described.

1.4 Case considerations malfunctions of safety-critical software

Safety-critical software has always been seen as automatically requiring higher standards throughout all development stages; from gathering the requirements, to carefully building the specifications, developing and implementing the software. Similarly, the verification and validation procedures are rigorous and following the desired safety-critical behavior, taking into consideration time and cost.

Moreover, a straightforward, seemingly harmless system can lead to life-threatening circumstances when used in a critical chain. For example, in flight control software, it could lead to plane crashes and life losses. Whereas, in healthcare, it could lead to a possible delay with a critical treatment. Imagine a hospital information system that does not notify a patient to follow-up to a critical consult, or a medical robot that malfunctions, this puts the patient's life at risk. In both cases, the risk escalates because of the wide install base of such software.

In the usual development process, the software can be patched on a constant basis, without much emphasis on quality upfront. Improving the quality of an imperative product becomes life-practice during its lifecycle by patch working. In addition, when adopting agile management practices, it is very relevant for software engineering teams to face the challenges of constant improvement with limited iterations and requirements. Next, the question for safety-critical software systems regards the patching aspect. In contrast to conventional delivery times of a software patch, which can be measured even in hours, the switch to safety-critical software will generally require re-entering of the certification cycle, especially after a fatal accident. It is a time-consuming, and sometimes expensive, process, which is definitely not quickly fixed.

This section addresses problematic implementation of software that led to a mass recall of products, closing business units and catastrophic outcomes.

First three cases are introduced:

1.4.1 CASE 1: Boeing 737 MAX flight control software malfunction

In the 50 years since its first flight, the Boeing 737 MAX had an exceptional safety record. Recently, Boeing opted to introduce fuel-efficient engines for the model 737 MAX. The change resulted in a weight redistribution of the plane. Instead of redesigning the fuselage to generate a proper weight distribution, Boeing introduced a flight control software module assisting the landing procedure for stabilizing the plane. However, because of a landing sensor failure and a software design error, the pilots lost control of the plane while stalling. Investigators confirmed that the transmitted information from a single sensor, in both accidents, caused the flight control system to strongly descent the jet's nose, ultimately leading to a steep, deadly dive. Simultaneously, because of the software error, pilots could not take control of the plane, resulting in the loss of 346 lives in two different plane crashes. Important now is how the engineering lessons of failing safety-critical systems are integrated into the software industry, to prevent catastrophic outcomes.

Authorities explained that Boeing, during the certification procedures, disregarded the automated stall prevention feature as a critical system that could lead to potential loss of life. Classifying the stall-prevention behaviors as a critical feature would have led to further scrutiny. If engineers and mid-level managers referred to Boeing's early classification for security and critical behavior with more scrutiny, these automatically potential risks would have been further analyzed. Whereby mitigation actions could have been arranged to handle those specific risks.

Eventually, the Boeing aircraft fleet was grounded until the software issue was resolved. In the process of grounding the fleet, 1 billion dollars in terms of losses were registered. Note, any time or money investment for identifying such critical behaviors beforehand would have saved lives and be exponentially cheaper than handling it afterwards.

1.4.2 CASE 2: Medtronic chamber pacemakers recall

Because of the extensive volume of the install base in healthcare informatics, safety control software errors can pose threats and higher liabilities.

Reading the information that the FOOD and Drug Administration (FDA) published in January 2019, Medtronic, Inc. Dual Chamber Implantable Pulse Generators (IPGs) had to be recalled from the market. The IPGs are implanted cardiac pacemakers, which provide stimulation to increase the heartrate of patients with a slow heart rhythm (bradycardia) or no heart rhythm. In Figure 1. Medtronic has issued an urgent medical device recall

and distribution suspension for the dual chamber pacemakers, which had a worldwide coverage.

The screenshot shows the Medtronic website header with the logo and 'United States' dropdown. The navigation menu includes 'Patients', 'Professionals', 'Products', 'About', and 'Transforming Healthcare'. A search bar is located on the right. Below the header, a breadcrumb trail reads: 'Home > Healthcare Professionals > Products > Product Performance and Advisories > Urgent Medical Device Recall'. The main content area features a red heading 'URGENT MEDICAL DEVICE RECALL' and a sub-heading 'FOR A SUBSET OF MEDTRONIC DUAL CHAMBER PACEMAKERS'. The date 'January 2019' is displayed. The salutation is 'Dear Physician or Healthcare Professional,'. The body text begins with: 'This letter is to inform you of a voluntary recall and distribution suspension affecting a subset of Medtronic dual chamber pacemakers distributed worldwide between 10 March 2017 and 7 January 2019 under the brand names Adapta™, Versa™ and Sensia™. Please note that not all devices within these brand names are affected by this recall. This letter contains a description of the issue and programming'. A printer icon is visible on the right side of the page.

Figure 1 : Medtronic press release - pacemaker recall 2019

The pulse generator is the small implanted unit containing the battery and other electronic parts. These devices are designed to be used in addition to routine clinical monitoring by a health care professional. The reason for the recall stated was: “due to the possibility of a software error that can result in a lack of pacing. Patients and physicians cannot predict whether and when this software error might occur. A lack of pacing could result in patients experiencing slow heart beating, low blood pressure, and symptoms such as lightheadedness, fainting, and even death.”

When an implantable device can malfunction because of a software issue, and can lead to a patient’s death, the issue becomes severe. Medtronic had to recall 13,440 devices distributed throughout the United States. They stated that a software update was developed, which could be installed on affected devices to correct the issue. Meanwhile, Medtronic requested doctors to return all unused and unopened devices. Moreover, they warned patients if new or unexpected symptoms appeared with a pause in pacing, they should immediately approach their usual medical care. Medtronic was obliged to provide mitigation actions towards this issue. Note, since they could not provide remote servicing, they had to recall products of the market and make the issue public to safeguard the patient’s wellbeing.

1.4.3 CASE 3: Philips Cleveland FDA investigation

Furthermore, Philips Cleveland has put patients’ lives at risk by medical software and products manifesting malfunctions. In this case, when the FDA intervened, with more drastic measures to the point that the Philips Cleveland business unit had to be

closed. Therefore, the focus within Philips Cleveland switched to training and research only (FDA, 2019).

According to the report from FDA, there were 133,845 complaints. 97% complaints were closed based on the assigned hazard harm matrix symptom codes. From the 3,623 remaining complaints, 1,792 of these should have been transferred to Philips complaint handling unit for further investigation based on the company's own work instructions.

The 2017 report was only the endpoint of a series of reports issued by the FDA that concerned the Philips mitigation of risks and quality aspects at the Cleveland production facility. Even if Philips continuously invested to improve these aspects, it served as a valuable lesson, regarding implementation of software medical devices. In the process, Philips improved the quality systems, and their procedures and accountability in the process when dealing with the extensive number of nonconformities. Philips learned to use these lessons across the company worldwide; therefore the failure to reach the high quality that Philips is known for, generated other winning scenarios. To deal with the reputation loss, in 2017 after a long history of nonconformities, Philips had to take drastic measures to the point of closing the production facility and focus only on research and development in Cleveland.

In Figure 2, you can observe the first page of the 2017 FDA report that contained 18 pages, describing quality control issues and various other nonconformities, which could lead to potential serious injuries or potential death.

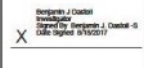
DEPARTMENT OF HEALTH AND HUMAN SERVICES FOOD AND DRUG ADMINISTRATION	
DISTRICT ADDRESS AND PHONE NUMBER 6751 Steger Drive Cincinnati, OH 45237-3097 (513) 679-2700 Fax: (513) 679-2772	DATE(S) OF INSPECTION 7/17/2017-8/18/2017* FBI NUMBER 1525965
NAME AND TITLE OF INDIVIDUAL TO WHOM REPORT ISSUED Lakshmi N. Gudapakkam , Business Leader and Senior VP CT/AMI	
FIRM NAME Philips Medical Systems (Cleveland) Inc	STREET ADDRESS 595 Miner Rd
CITY, STATE, ZIP CODE, COUNTRY Cleveland, OH 44143-2131	TYPE ESTABLISHMENT INSPECTED Medical Device Manufacturer
This document lists observations made by the FDA representative(s) during the inspection of your facility. They are inspectional observations, and do not represent a final Agency determination regarding your compliance. If you have an objection regarding an observation, or have implemented, or plan to implement, corrective action in response to an observation, you may discuss the objection or action with the FDA representative(s) during the inspection or submit this information to FDA at the address above. If you have any questions, please contact FDA at the phone number and address above.	
<i>The observations noted in this Form FDA-483 are not an exhaustive listing of objectionable conditions. Under the law, your firm is responsible for conducting internal self-audits to identify and correct any and all violations of the quality system requirements.</i>	
<p>DURING AN INSPECTION OF YOUR FIRM WE OBSERVED:</p> <p>OBSERVATION 1 Complaints involving the possible failure of a device to meet any of its specifications were not reviewed, evaluated and investigated where necessary.</p> <p>Specifically, you are not adequately investigating complaints. For example:</p> <p>A.) Out of 133,845 complaints received from July 2016-July 2017, 129,736 complaints were closed based only on the assigned HHM (hazard/harm) symptom code and not further investigated (97%). From January 2016 to present, there were 3,623 complaints (representing 33 HHM symptom codes) that received a low HHM severity level of (b) (4) (less than moderate or no injury), but had a high RMM (risk matrix) severity level (b) (4) potential serious injury or (b) (4) potential death).</p> <p>Of these 3,623 complaints, 1,792 should have been escalated based upon your "<u>Service Record Reviewer Team (SRRT) Monitoring Work Instruction</u>", #CNV-073105-01 and forwarded to the Complaint Handling Unit (CHU) for further investigation.</p> <p>Additionally, a query of complaints from Feb 2014 to present for HMM codes related to rescan or reinjection of patients found that codes which meet the criteria for escalation are not always forwarded to the CHU. For example:</p> <p style="text-align: center;">AMENDMENT 2</p>	
SEE REVERSE OF THIS PAGE	EMPLOYEE(S) SIGNATURE Benjamin J Dastoli, Investigator Teresa K Kastner, Investigator Christina L Bigham, Investigator Laureen M Geniusz, Investigator
	
DATE ISSUED 8/18/2017	
FORM FDA 483 (09/08)	PREVIOUS EDITION OBSOLETE
INSPECTIONAL OBSERVATIONS	
PAGE 1 OF 18 PAGES	

Figure 2 : FDA Investigation report for Philips Cleveland

Software issues generated recalls, in the Philips Cleveland case. In the indicated sample, there were 1890 Tomography X-ray systems with the same deployed software bug, with class II recall action. This generated an extensive recall strategy based on quality and software related developments.

Date Initiated by Firm	June 07, 2017
Create Date	October 31, 2018
Recall Status ¹	Open ³ , Classified
Recall Number	Z-0304-2019
Recall Event ID	81403
510(K)Number	K171850
Product Classification	System_x-ray_tomography_computed - Product Code JAK
Product	Brilliance 64 (Model No. 728231), Software version 4.1.6 Product Usage: Computed Tomography X-ray systems intended to produce cross-sectional Images of the body by computer reconstruction of X-ray transmission data taken at different angles and planes. These devices may include signal analysts and display equipment, patient and equipment supports, components, and accessories.
Code Information	Software Version 4.1.6
Recalling Firm/ Manufacturer	Philips Medical Systems (Cleveland) Inc 595 Miner Rd Cleveland OH 44143-2131
For Additional Information Contact	Ms. Holly Wright Lee 440-483-2015
Manufacturer Reason for Recall	It was reported that scanners running certain software versions provide confusing information in the "Impressions" section of the Calcium Score report. The generated report provides multiple analyses of the amount of plaque detected, as if they all apply to the patient at the same time. This misleading guidance can be potentially misleading to the user, and may lead to mistreatment of the patient.
FDA Determined Cause ²	Software design
Action	The recalling firm sent Customer Information letters dated June 7, 2017, to affected customers. The letter notified customers of the product issue. Customers were instructed to determine whether they had a potentially affected system by checking the software version of their device. Customers were reminded that the "Impressions" section of the report is not intended for diagnostic use. Users should instead focus on the total calcium score shown in the "Findings" section, the coronary artery score(s) and/or the "Age and Gender" graph as identified in the Instructions for Use (IFU). The firm sent a follow-up dated July 3, 2018, to inform customers that software updates had been released which resolved the issue. If you need any further information or support concerning this issue, please contact your local Philips representative: For North America and Canada, contact the Customer Care Solutions Center (1 -800-722-9377 and follow the prompts).
Quantity in Commerce	1890
Distribution	US Nationwide Distribution
Total Product Life Cycle	TPLC Device Report

Figure 3 : Philips Cleveland FDA recall - software design cause

The firm's diagnostic imaging manufacturing operations in Cleveland "currently make up less than 3% of the total global diagnostic imaging sales volume, ceased fully in the second half of 2018. Philips now plans on investing in a new R&D facility in Cleveland." (Philips, 2018) according to Steve Klink. As Philips retains a high standard towards its products, and because of the extensive losses in the Cleveland business unit, the management in Philips decided to close the business unit altogether and focus only on the R&D Facility.

1.4.4 Impact - FDA Volume recall analysis for software

When a company learns that one of its medical devices is problematic on the US market. it offers correction or removal, depending on the nature of the recall action to be taken by the supplier, and requires so before FDA needs to do an investigation about the filed

complaint. This response is related to the internal customer service process that the company has in place.

The company has either the possibility to perform correction actions that address a signaled problem with a medical device that is being used or has been sold. Alternatively, it has the possibility to remove the medical device from the customer premises, or at the same location.

FDA uses the term "recall" to address a problem with medical devices, which violate the FDA law when a manufacturer takes correction or removal measures. Recalls occur if the medical devices are faulty, if they may be a health risk, or if they are both faulty and retain a potential health risk.

Recalling a medical device does not always imply that you have to stop using the product or the mandatory action to return the product to the manufacturer. Recall sometimes involves the checking, adjustment, or fixing of the medical device. The FDA may legally require an enterprise to retract a device. This could be the case if an enterprise continues to refuse to recall a device linked to serious health problems or death.

Class I: A situation where there is a reasonable chance that a product will cause serious health problems or death.

Class II: A situation where a product may cause a temporary or reversible health problem or where there is a slight chance that it will cause serious health problems or death.

Class III: A situation where a product is not likely to cause any health problem or injury.

Let us consider the following analysis made using data offered by the U.S. Department of Health & Human services portal, from the FDA Section provided information for medical device recalls.

The database can be filtered by Product Name, Product Code, Recall Class, Recall Date, Recall Number, Reasons for Recall, Recalling Firm, and Root Cause. Based on the patient harm, classes were introduced, to classify the 3 scenarios. Each of the recall for software issues had an essential identified root cause. There were five identified root causes by software: Software Design, Software Design Change, Software Design Change in the Manufacturing Process, Software Change Control, and Software in the Use Environment.

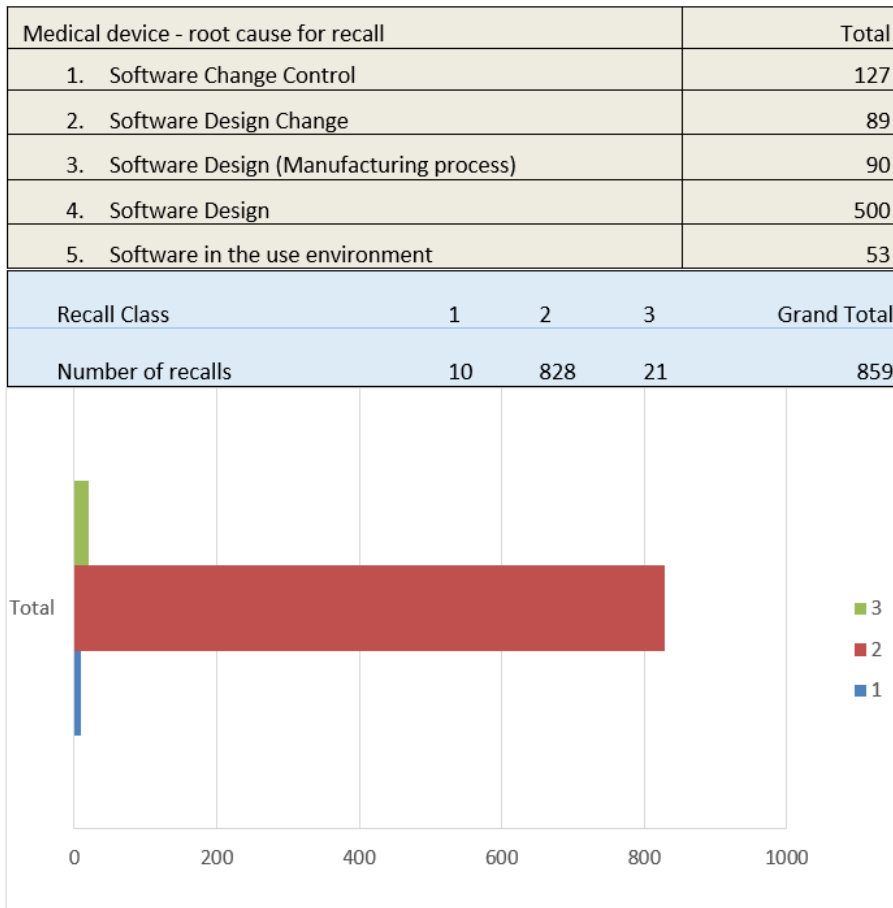


Figure 4 : FDA class distribution of software recalls

The sum of the total software issues related recalls by FDA equals 859 recalls. From the 859 recalls, only 21 were for minor reasons that would not lead to patient harm. The 828 recalls were being identified as class 2. These recalls concerned software problems that would lead to short-term health problems, with a minor chance to cause serious injury or death. The last 10 recalls were being identified as class 1, due to the chance to lead to health damage or loss of life. Another aspect that should be considered, because of the economy of scales, is that the software issues can be traced to several thousand devices. Only one instance for a software recall is traced to all the devices on which the software was installed, which in some cases implies tremendous post sale costs for the mitigation actions.

1.5 Philips VitalHealth company profile and products

Philips leverages its rich heritage of innovation as one of the world’s largest developers of healthcare technology. For the overall sales volume, EUR 1.7 billion are dedicated to

research, supporting 7,000+ engineers in development of future technology enabled healthcare solutions.

“Philips acquired VitalHealth Software, a software company whose mission is to contribute to the improvement of global healthcare through innovative IT-solutions. For that purpose, a platform has been developed which has large potential within healthcare organizations. VitalHealth Software was founded in 2006 by Mayo Clinic (USA) and Noaber Foundation (the Netherlands). The company was founded to develop game changing cloud-based eHealth solutions with emphasis on solutions for people with chronic diseases such as Diabetes, COPD, CHF, Depression, Cancer and Alzheimer's.” (VitalHealth, 2019)



VitalHealth Suite - Integrated Population Health Management Platform

Figure 5 : VitalHealth platform

To enable team-based population health, Philips proposes to introduce an end-to-end population health management and care suite of software, VitalHealth, for all care-related interactions with the individual, as well as for population analytics and stratification, and outcomes tracking and management. VitalHealth is currently used by 6 million patients and 132,000 professionals across more than 170 provider networks around the globe. Philips VitalHealth has customers in the United States, the Netherlands, China, Sweden, Finland, India, France and Belgium.

VitalHealth consists of solutions covering four focus areas:

- 1) Patient and clinician engagement, (ENGAGE)
- 2) Care coordination, (COORDINATE)
- 3) Outcome measurement & management (QUEST LINK)
- 4) Population Analytics. (INSIGHT)



Figure 6 : Philips VitalHealth products

1.5.1 ENGAGE - Patient and clinician engagement

“The VitalHealth solutions encourage patient engagement through use of interface with a base EMR patient portal or use of the VitalHealth patient portal. Individualized care plans, based upon best practice care paths, include a set of activities that can be automatically assigned to the patient. These activities are based upon the goals of the patient. Completion of activities/tasks and progress towards individualized goals can be automatically assed with alerts/reminders sent to the patient or their care giver” (VitalHealth, 2019).

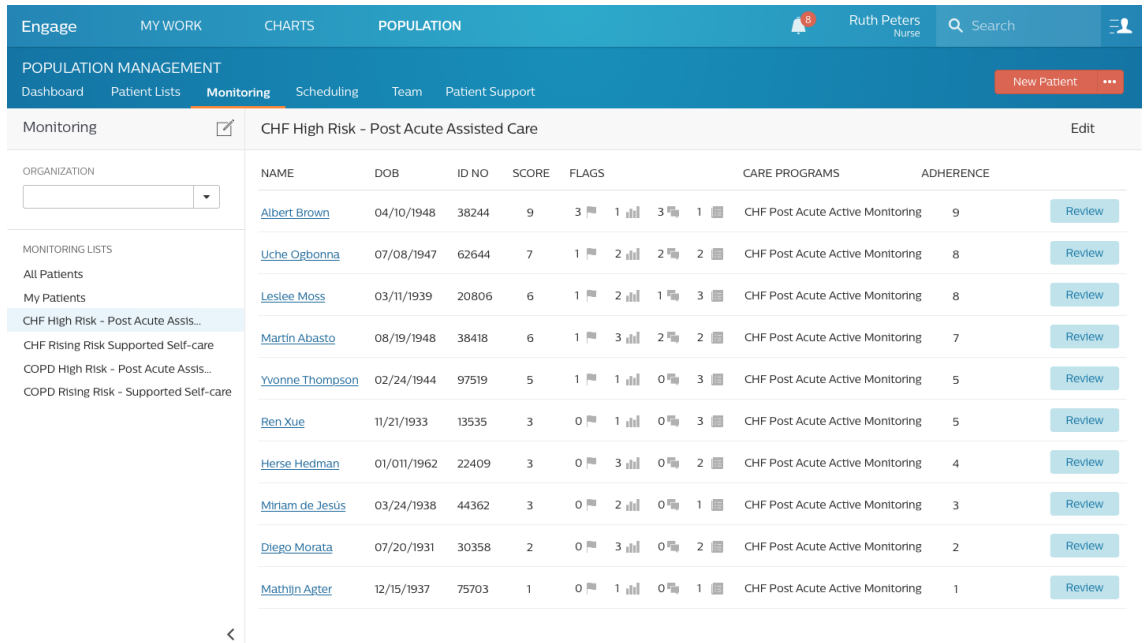


Figure 7 : Population health management portal

Features:

- Potential to determine the degree of patient activation at the onset of their care
- Continuous automatic monitoring of the individual patient’s response to assignment
- Remote self-monitoring with functionality to record patient specific data
- Integrated for easy online collaboration between professional and patient
- User friendly interfaces for use of mobile devices
- Personalized (online) education

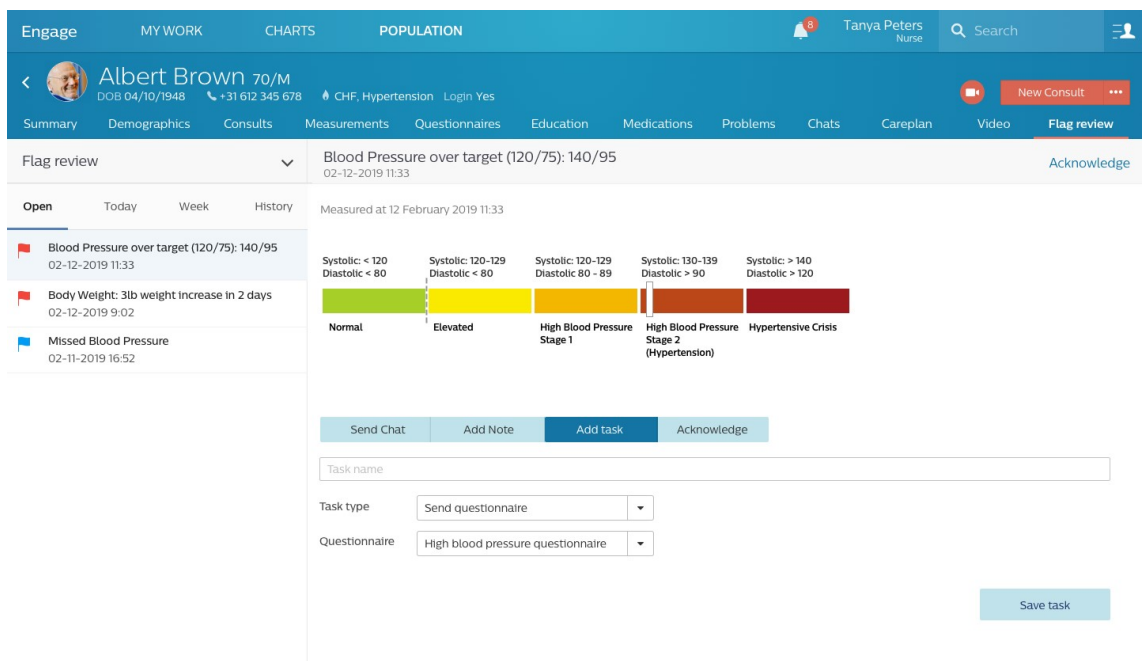


Figure 8 : Patient portal

“The VitalHealth Patient Engagement solutions ensure that patients participate in a timely manner in shared decision-making, supporting better health outcomes. These solutions support the assignment of individualized care plans based upon best practice care pathways and patient preferences. Shared decision-making is supported leading to higher levels of patient engagement and improved outcomes” (VitalHealth, 2019).

1.5.2 COORDINATE - Care coordination and care management

“The growing global burden of chronic disease is forcing providers and health care systems to deliver the care they provide in new ways. Communication amongst providers and between providers and patients is central to achieving better outcomes at lower costs. VitalHealth Software’s approach to Care Coordination facilitates this new paradigm of health care delivery – team-based care.

VitalHealth Care Coordination facilitates integrated collaboration within multidisciplinary care teams. It allows for better, more effective and more transparent care for these patients. Our solutions support collaboration and communication between involved healthcare professionals and other stakeholders within the ecosystem. The automated delivery of reminders and alerts facilitates not only the communication between care providers but also decision support and it ensures that care givers and other stakeholders with appropriate expertise (e.g. fitness coach) can efficiently participate in the care process within the ecosystem” (VitalHealth, 2019).

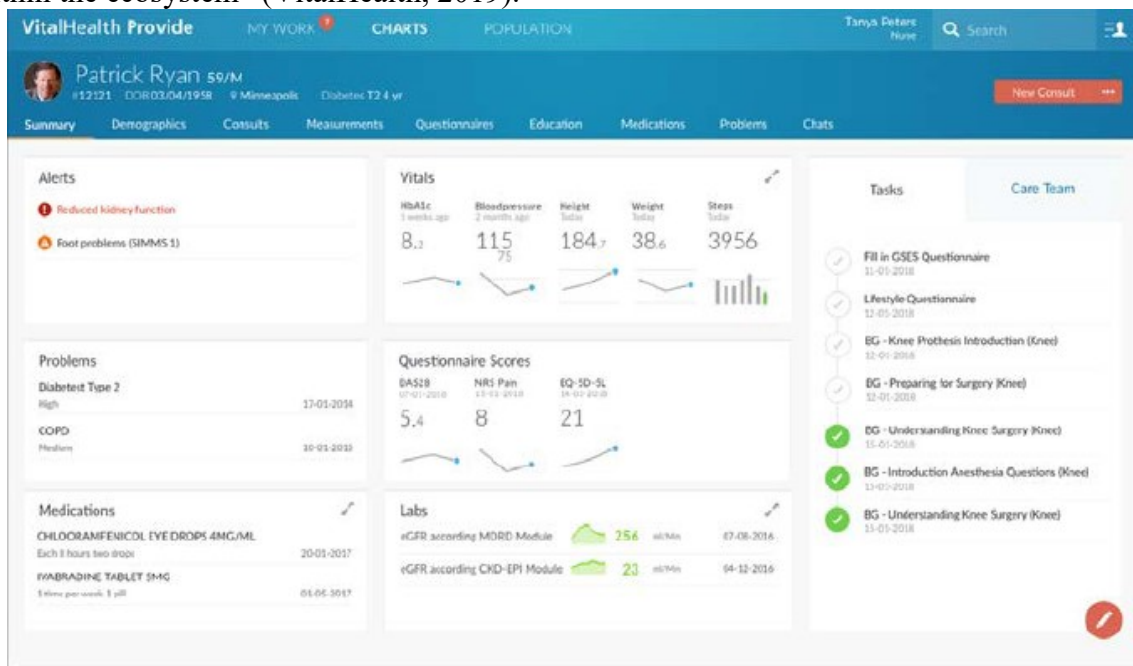


Figure 9 : Care coordination portal

“Managing chronic conditions is effective and efficient with VitalHealth’s Care Coordination solutions. Disease specific content, including care pathways, is available for the

common chronic conditions including Asthma, COPD, Diabetes, and Behavioural/Mental Health. The disease specific care pathways are individualized into care plans for each patient, with role-based assignment of tasks. This allows stakeholders to work together as a care team within the ecosystem to provide holistic guidance and care. The VitalHealth solutions include tools to improve patient engagement, individualize the manner in which they participate in shared decision making and provide remote monitoring” (VitalHealth, 2019).

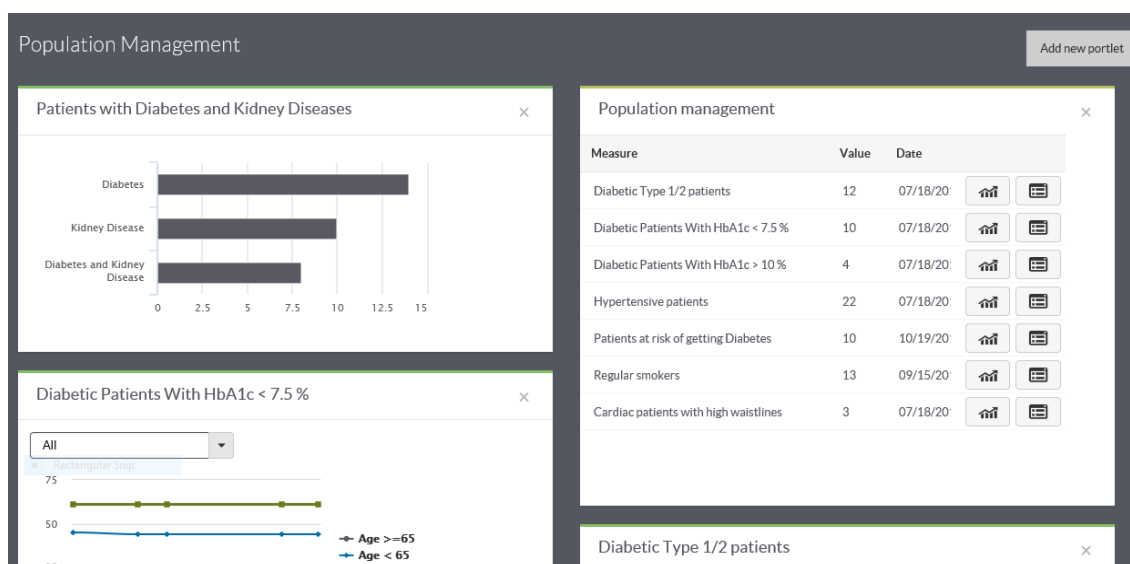


Figure 10 : Population health management view

The following are the features in this software:

- User-friendly and easily configurable dashboards
- Individualized and best practice-based care pathways
- Personalized care plans
- Built-in clinical decision support, based on (medical) guidelines
- Referral Management
- Care Pathways
- Remote monitoring
- Care team support
- Two-way EMR integration
- Automated rules-based evaluation of patient responses
- Automated alerts

1.5.3 QUESTLINK - Outcomes management

“Outcomes are what matters to patients, providers and payers, and the overall ecosystem. Recently, systems to support the efficient collection of outcomes have become even

more important as reimbursement has been linked to measurable outcomes. VitalHealth Software solutions support the efficient collection of outcomes data. The configurable rules based approach automates the collection of the outcomes data and use of that data to improve individual patient care and guide the development of the ecosystem.

VitalHealth's Outcomes Measurement solution supports hundreds of validated survey instruments. Many of these instruments are required for reimbursement by payers including CMS. The ease, with which these surveys can be automatically sent, based upon diagnostic or procedural codes, helps to ensure that providers and health care systems minimize the administrative burden related to outcomes measurement. Outcomes data can also be helpful in identifying quality improvement opportunities for health care systems. Together we can continuously improve the care we provide" (VitalHealth, 2019).

1.5.4 INSIGHT - population healthcare analytics

"Population management is based upon the evaluation of outcomes for groups of defined individuals. Care is delivered one patient at a time. To improve outcomes for populations we must improve the outcomes for individuals. Therefore, VitalHealth Healthcare Analytics solutions enable providers and systems to both monitor individual outcomes and the outcomes for appropriately risk stratified populations. Our solutions enable health care systems to flexibly evaluate outcomes of populations which are important to the organization. This would help provide evidence-based information about the ecosystem and guide decision-making.

VitalHealth Healthcare Analytics solutions offer data mining tools and process mining algorithms. This helps health care systems and providers improve their population health outcomes based upon an iterative process of evaluation of appropriately risk stratified groups. The process is based upon individual actionable care plans linked to flexibly configured outcomes measurement" (VitalHealth, 2019).

The following are the features in this software:

- Risk Stratification
- Outcome Analysis
- Data Mining

1.6 Regulation requirements – European union regulatory environment

Introduction for regulatory strategy

Creating a better legal structure is probably the most important way to protect users from software abuse (Rutkowski, 2014). Regulators around the world organize to generate harmonized standards. Besides these harmonized standards, in practice, governments develop own country-specific regulation that software manufactures have to abide by in order to gain market access. The controller processes healthcare data within strict compliance rules. Whereas information around health and treatment will be regarded as a secret. The healthcare organization is keeping individuals fully informed about the purpose of sharing data for an intended purpose asking for explicit consent. Maintaining data securely is increasingly difficult for highly sensitive information. Therefore, update policies and procedures around the collection, storage and use of patient data becomes a critical practice (Fuentes 2018). Healthcare organizations handle data varying from financial records and health insurance information to patient test results and biometric information. This data is uniquely linked to an individual and are mostly unalterable (Fuentes 2018).

To safeguard healthcare practices and ensure the quality and integrity of the healthcare act, regulation has been adopted to govern over patient rights. Regulation also dictates under what rules, and limits software in healthcare operates. In addition, it is important to specify that regulation can be region and country specific, so in order to gain market access, a healthcare software needs to abide by the specific regulation of that region and country.

The two regions that have extensive regulation that extend to healthcare software are United States and Europe. FDA is the main regulator for the US. The European Commission is the regulator for the European Union. It is usually easier to gain market if you have a product certified in either US or Europe due to commercial agreements and harmonized international standards. Moreover, there are countries that have commercial international agreement to facilitate trade between states. When this is the case the certification process can be faster and cheaper, and market access becomes easier to obtain.

Therefore, the rational to gain regulatory approvals into US and Europe, becomes a winning one. In this report, only the European Union Regulation was treated, given the fact that Philips VitalHealth products, started in the Netherlands. In addition, the scenario became more relevant for Philips VitalHealth because of the new changes made in the European regulations.

1.6.1 European union medical device regulation (EU MDR)

In the European Union (EU), healthcare software is classified as a medical device and therefore must abide by medical device regulation. Philips VitalHealth has software classifiable as class 1 and 2, according to the new EU Medical Device Regulation (EU MDR). The EU has a medical device directive (MDD) in place that is establishing some limitations and guidelines for healthcare products and medical devices. From 2020, a new policy will be applied within the EU that will regulate the medical device market with mandatory immediate action (European Commission, 2018). EU MDR requires more constraints for medical devices. Therefore, it ensures more quality and safety for devices used in healthcare. Each country has a regulation body: Philips VitalHealth resides in the Netherlands and can choose different regulators for medical devices. For the VitalHealth product certification the choice was TÜV SÜD. TÜV SÜD has arranged a timeline that medical device suppliers including Philips VitalHealth could follow while having to abide by the recommended deadline and practices. (TÜV SÜD, 2018)

EU MDR Implementation Timelines 2017-2025

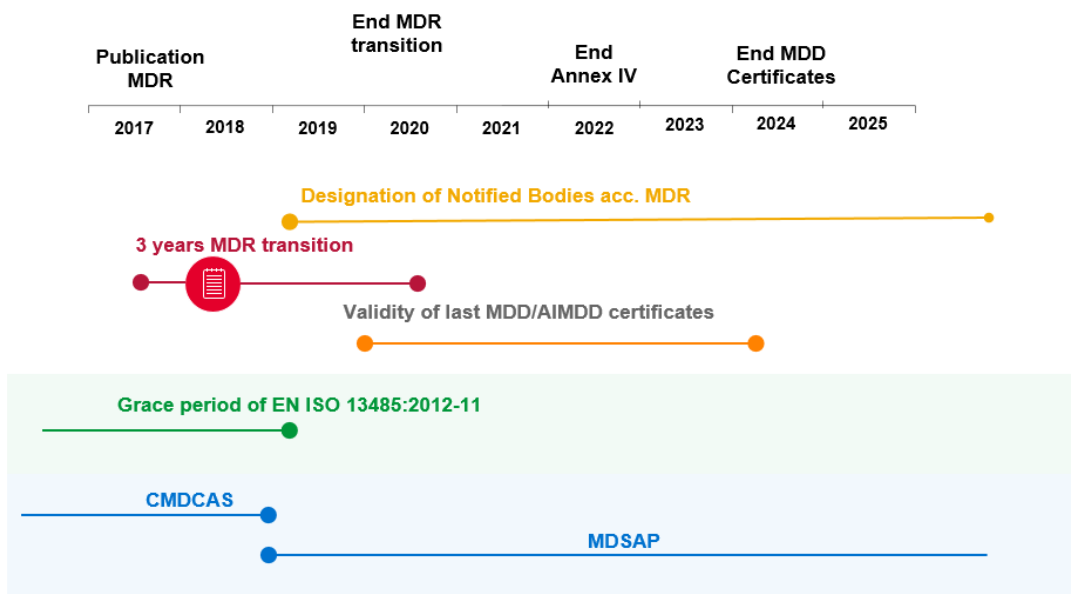


Figure 11 : TÜV SÜD- EU MDR Milestones for Philips VitalHealth

Milestone: May 5, 2017,

- New medical device regulation was published with a transition period of 3 years.

- Due to this fact and the fact that this regulation includes specific clinical requirements which are not consistent with the EU MDR Guidance Document on clinical evaluation
- In the Netherlands TÜV SÜD decided to extend the implementation timeline for the reflection of the state-of-the-art methods of clinical evaluation. This decision was taken to allow medical device manufacturers to use their resources effectively when adopting the upcoming changes with the new regulation to their clinical evidence documentation.
- extension is just possible if the requirements on clinical evaluation and active post-market surveillance of the applicable directive MDR

Milestone: July 31, 2017 – May 25, 2020

- Every submission can still follow the currently used methodology reflected in the EU MDR or another comparable method
- Every submission shall include a plan on how to reflect the current state-of-the-art method for clinical evaluation
- Every technical documentation that is selected in this period shall either include a plan for the reflection of state-of-the-art methodology implementation as presented, for example, in the, or be part of a general plan of the manufacturer

Milestone: May 26, 2020

- Clinical Evaluation Report shall be reflecting the current state-of-the-art method of clinical evaluation by either following the EU MDR revisions or another comparable method

In order to reach these milestones because of the complexity of the certification process, a stepwise approach needs to be arranged focusing on the main action principles explained in the EU MDR document and annexes (TÜV SÜD, 2018) :

- A. Checklist against the EU MDR regulation (if applicable as a medical device)
- B. Identify class rules – conformity assessment routes in the EU MDR
- C. Identify risk level – risk profile
- D. Conformity assessment routes and essential principles
- E. Certification of the quality management system
- F. Product certifications
- G. Product lifecycle management

Based on the EU MDR document and annexes, you can follow fragment statement from the regulation. For action A. Check against EU MDR regulation (if medical device)

according Philips VitalHealth product white paper Philips VitalHealth products are a medical (You can see underlined the reasons by which the software products become medical devices).

Medical device definition

“(1) ‘medical device’ means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

(2) Diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, or compensation for, an injury or disability,

(3) Investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, ...” The Phillips VitalHealth software products fall into the class category IIa and IIb, according to annex VIII.

Device Class	CA procedure	MDR certificates
IIa	Chapter I + III of Annex IX and section 4 of representative device	EU quality management certificate + EU technical documentation assessment certificate

Table 1 : Classification EU MDR

From EU MDR regulation article 6.3. Rule 11:

Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause:

death or an irreversible deterioration of a person's state of health, in which case it is in class III; or

a serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as class IIb.

Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring of vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb. All other software is classified as class I.

1.6.2 Product and QMS Certifications for Philips VitalHealth

It is crucial when thinking about product design and development to have higher standards in mind. If the product is certified against higher standards, the ability to sell and be compliant to client needs is strongly facilitated. The use of harmonized standards, becomes very relevant, because they enforce client trust on international level also making the regulatory approval a faster process.

Harmonized standards are available for:

- Quality management systems (QMS)
- Risk management
- Basic safety
- Usability
- Software development

For the EU harmonized standards are published in the Official Journal of the EU. Harmonized standards, including product standards need to be purchased (standardization organizations). At the beginning of a design and development cycle, the current regulatory requirement (and the customer needs/requirements) are gathered as input to the creation of the system requirements. Application of a harmonized standard gives the presumption of conformity to the Essential Requirements and GSPR.

Summary of Key Changes Impacting QMS Processes

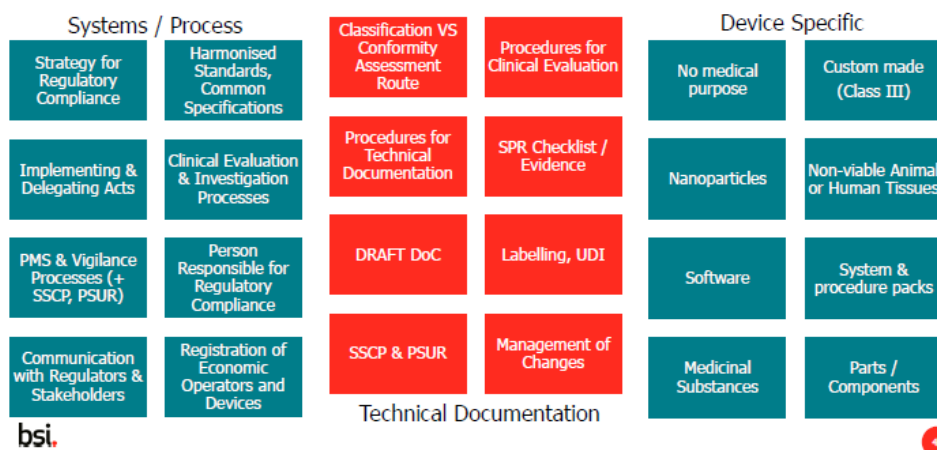


Figure 12 : Harmonized Standard EN ISO 13485 - QMS requirements

1.6.3 EU MDR Lifecycle approach

Relationship between device lifecycle, ongoing collection and monitoring of clinical evidence and requirements for vigilance and post market surveillance (PMS).

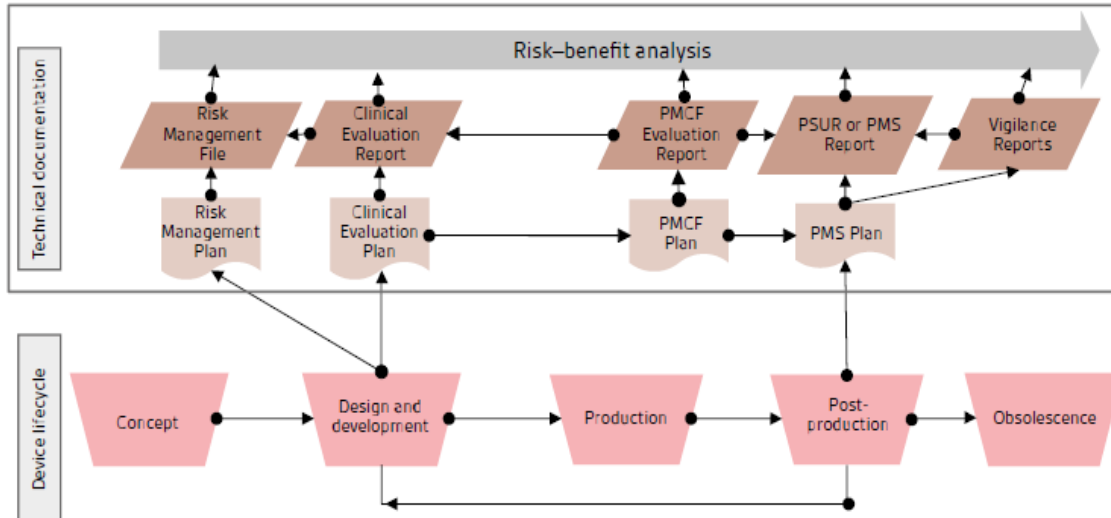


Figure 13 : Lifecycle approach - BSI Whitepaper

Two aspects to be taken into consideration, in lifecycle. The first one is related to the lifecycle stage: concept, design and development production postproduction and obsolesce. All of the above have technical documents that come out of each stage, that feed into the Risk-Benefit analysis.

1.6.4 General data protection regulation (GDPR)

Healthcare organizations inquire whether software companies comply with regulatory, security standards and deliver products that further allow the healthcare organization to comply with relevant regulatory standards and privacy laws. The healthcare organization becomes a data controller because it uses information systems to operate with patient data. The controller is the one who determines the purposes for which, and the way in which personal data is processed. By contrast, the software company is processing personal data on behalf of the data controller. The data processor is subject to far fewer obligations under the law. As a constant practice, the legal liability towards data subjects for controlling and processing patient data remains with the healthcare organization.

Controller - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor - The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data subject - The natural person whose data is being processed

- Personal Data: Any information relating to an identified or identifiable natural person ('data subject')/ Name, date of birth, IP-address, Mac Address; marital status, salary, etc.
- Special categories of personal data, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

According to GDPR regulations, ERP and IT systems have to maintain a refined IT Security and Risk Management procedures to ensure that the data is safe and not tampered with. GDPR enforces security measures when handling healthcare data, creating an extra layer of complexity over healthcare assets. Information about healthcare assets is highly sensitive and considered as a special category altogether (Zarsky, 2017).

1.6.5 European Interoperability Framework (EIF)

The interoperability between systems and different administrative levels is enforced within the EU by the European Interoperability Framework (EIF). Trust is linked with aspects like confidentiality, integrity, accountability, authenticity, identity, and data management.

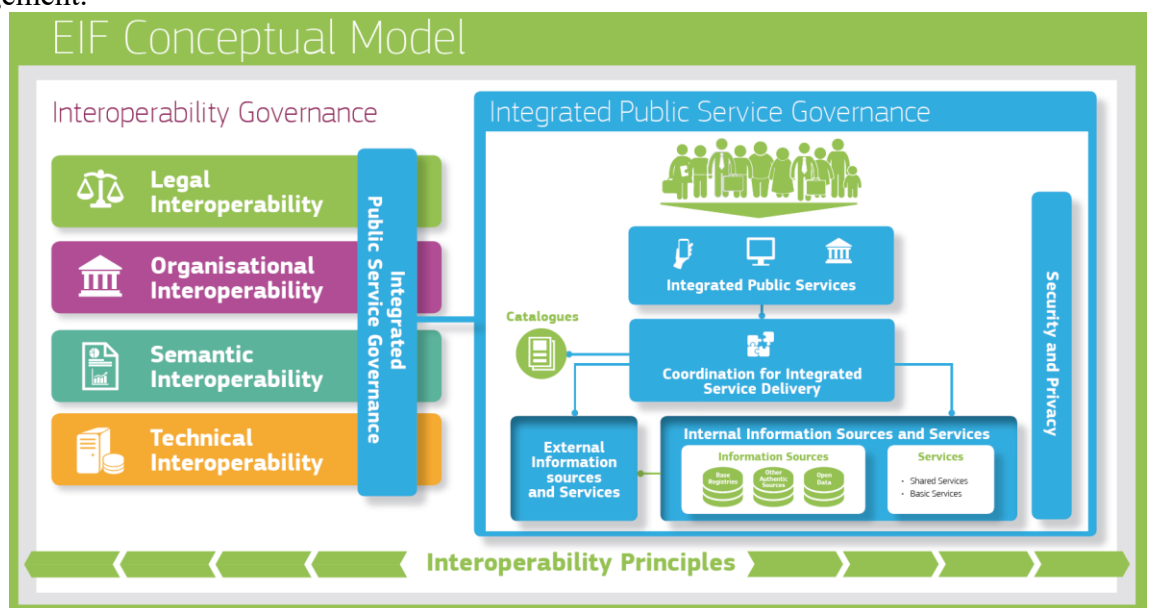


Figure 14: European interoperability framework concept

The renewed European Interoperability Framework (EIF) was adopted on 23 March 2017, approximately one year before the GDPR was applied. EIF gives specific guidance on how to create interoperable digital public services. It has 4 levels of interoperability, 12 underlying principles, and 47 concrete recommendations on how to improve governance on their digital platforms. The four levels of interoperability consist of the legal, organizational, semantic, and technical interoperability. EIF is a key instrument for establishing interoperable digital services not only at EU level, but also at national and regional. Enhancing the consistency of operations among different stakeholders, through healthcare IT, makes this Framework relevant to be adopted in the following years. Public administrations can save time, reduce costs, increase transparency and improve the quality of services (European Commission, 2017). Even though the EIF is just the European Commission's recommendation, the benefits of implementation incentives encourage organizations to start using the framework within their systems.

1.7 Risk management & control for software in healthcare

It is generally understood that a risk is a combination of the probability and the severity of the harmful issue happening. Nevertheless, it is difficult to reach common understanding between various stakeholders about the application of risk management as each party sees various potential threats, and considers a different probability and severity to each threat. Regarding software in healthcare, the protection of the patient by managing the risk to quality must be taken as paramount, although there are many actors involved. The actors vary from the patient to the physicians, and the government regulation and industry services.

The quality risk management is only one part of the overall risk. The quality risk combined with security and privacy offer a more comprehensive risk profile for software in healthcare. It is important to understand that product quality should remain aligned with the attributes used in clinical trials during the entire product life cycle. An effective risk management approach for quality can also guarantee the patient the high-quality healthcare act. The recommended practice is a proactive way of identifying and controlling potential quality issues during design and development of software in healthcare. The use of quality risk management can further improve decision-making if there is a quality problem.

In healthcare informatics there are three main types of risks identified based on the critical behavior that software should deliver. Security and privacy are the first two, and both of them enforce user trust and integrity of the medical act. The third risk is related to the usability of the software and the probability to generate patient harm. Identifying

the critical behaviors for medical software is crucial in the early design phases. As described in the literature review, risks related to privacy and security are handled in the design phase. Thus, security and privacy by design come as a mandatory practice. In the next subchapter, mandatory regulatory aspects are discussed.

Especially in healthcare software, the risks related to patient harm occur from the extended usage of the software itself. Usability related risk analysis is relevant to be build. The source of a potential hazard is identified and described, this based on the usability standard. All of the events, that make the hazard occur, are mapped. The hazardous situation is described and linked to the patient harm profile.

Initial Risk			Mitigation / risk control measures	Patient Harm	Verification/validation reports <i>(medical device / clinical study only)</i>	8. Residual risk			Residual risk acceptable
Probability	Severity	Risk (S&P)	Mitigation description <i>(Describe the intended design changes or protective measures to lower harm probability and/or harm severity)</i>	Software safety class		Probability	Severity	Risk (S&P)	Add rationale when residual risk level is unacceptable, but the risk/benefit ratio is deemed acceptable.

Figure 15 : Risk control matrix for healthcare software

The risks need to be addressed and control measures need to be established. Each risk is treated individually, described and provided with an identifier. First, the initial risk is assessed in terms of probability and severity. Next, the probability can be categorized in frequent, probable, occasional, remote or improbable during normal use. Additionally, the severity can be categorized into five levels;

- catastrophic resulting in patient death,
- critical resulting in permanent impairment or life-threatening injury,
- serious resulting in injury or impairment requiring professional medical intervention,
- minor resulting in temporary injury or impairment not requiring professional medical intervention
- Negligible resulting in inconvenience or temporary discomfort.

Finally, a gateway control is put in place for acceptable and unacceptable risks. For the unacceptable risks, a mitigation action is assigned to them. A potential risk places the software in a completely different class in terms of regular consideration. The mitigation actions help to reduce the risks, but do not eliminate them completely. Therefore, there is still a residual risk that needs to be further mitigated. In some instances, the risk/benefit analysis can dictate if the risk is worthy to take because of the potential benefits for the business.

2 METHODOLOGY

The methodology chosen for this research was an exploratory-explanatory case study based on the problem statement and three-research questions. Exploratory methods were used to generate an in-depth understanding of business needs and current business practices. At the same time, the explanatory methods were relevant in presenting the desired results and the build-up using multiple artifacts information systems (IS) that answered the research questions.

As stated in the introduction, the following research questions were considered specific to the healthcare software product lifecycle:

- How to stay in compliance with regulatory requirements and export controls during the product lifecycle?
- How to present the regulatory regional information during the product lifecycle to the various stakeholders for medical serving software?
- How to ensure strategic business architecture to validate/grow/implement/ deliver value-added solutions with market access in a timely manner?

The research methods used to explore the product lifecycle of Philips-VitalHealth were data collection and data analysis. Meetings and interviews were planned and conducted on a weekly basis, to clarify and ensure the validity of the current information. Consistency was ensured by checking the current IS artifacts. During the interviews, an assessment based on the research questions was conducted for identifying new possible business practices.

The Philips VitalHealth IS artifacts were identified as constructs, and methods that were developed and used to support the business practice. Assessment of literature, regulations and roadmaps were also included in answering the research questions. In order to answer the research questions, new IS artifacts needed to be constructed. Following design science research, executive IS artifacts were built from the emerging knowledge process. In addition to design science, IS behavioral science research was used to inquire in the organizational process. Therefore, integrating newly acquired knowledge of software development cycle, new market entry, market access, quality control, regulatory control and change control, in the IS artifact. The IS artifact, in this case resulted to be the masterplan for product lifecycle management. The masterplan influences decision control over several aspects of the business, also offers strategic insights for roadmaps and future product development.

The aim of using the artifact, net benefits for the system service and quality of information. During several interviews both management and development and testing, expressed interest about its utility. The interplay between business strategy, IT strategy,

organizational infrastructure and IS infrastructure was addressed in the artifact creation. Implementation in a work system the objectives, tasks, problems and opportunities which defines business needs as perceived by individuals in Philips VitalHealth.

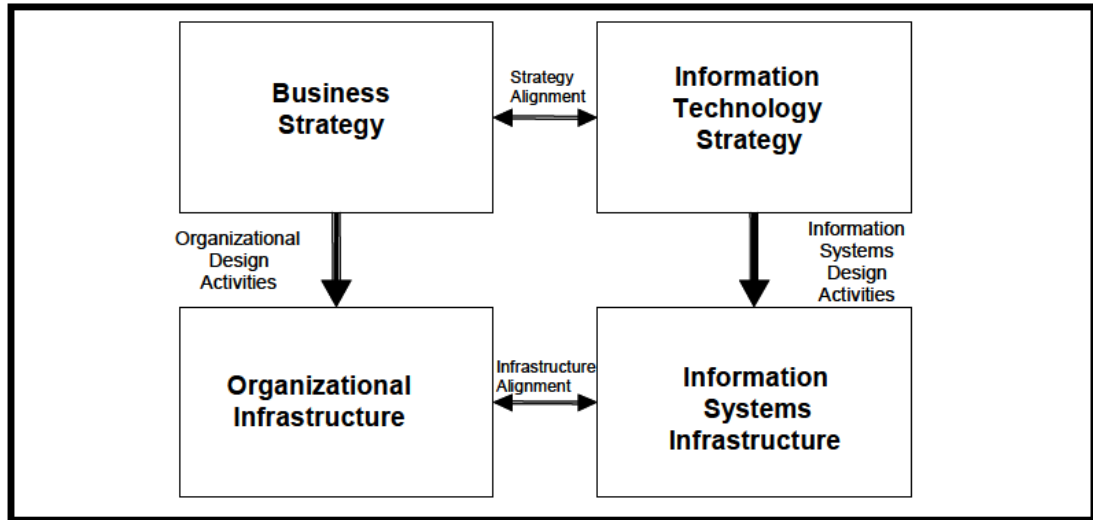


Figure 16: Strategic alignment: Leveraging information technology

The roles, skills, and characteristics of individuals in the organization shape such perceptions. In the context of corporate strategies, structures, culture and existing business processes, business needs were evaluated and assessed. Based on the research questions and the strategic alignment in Figure 16, information technology strategy mandated adapting to new IS artifacts to support the information systems infrastructure.

In the data collection stage from Philips VitalHealth the existing infrastructure for technology, applications, communication architectures and development capabilities were assessed. Identifying what is needed for the business to have market access, knowledge about regulatory aspects to sell the product on a new market was key to defining the problem statement and relevance of the research questions.

In the early iteration of the artifacts, the insights were gathered for each of the research question individually. They were compiled from technical documents, product development databases, compliance procedures, quality and regulatory requirements, legal agreements, audit tables, sales practices, and various product management tools. The purpose of the data collection was to collect all the relevant information into a product lifecycle masterplan.

This also implied gaining several layers of information with different complexity. Both a high-level picture and the in-depth rooted inquiry about the product lifecycle were relevant. The information collected in early stages was checked and verified with the people responsible over the process. For product lifecycle management, the relevant stakeholders were identified. They varied in roles from product managers, sales managers, quality and

regulatory responsible, developers to product testers and external consultants. Semi-structured interviews with stakeholders were conducted that could provide valuable input on how product development, requirement gathering, sales process, quality and regulatory controls shaped the Philips-VitalHealth product lifecycle management. In addition, not only the internal knowledge was gathered to ensure internal validity, but also the need for external validity of the evidence. External consultants were interviewed in order to find out from notified body/regulatory perspective what requirements are in place and what Philips VitalHealth needs to do in order to fulfill those requirements. Harmonized standards were introduced together with the external consultant on a roadmap of compliance standards. Based on the feedback loop intended as a practice in design science, to answer the research questions, three artifacts were created, compiling the relevant data and information. The main output was a design for a master plan for product lifecycle management for Philips-VitalHealth.

Methodologies are typically rooted in behavioral science data collection and empirical analytical techniques. On the basis of Hevner (2004), how design science is to be undertaken, assessed and presented, this section would describe the building of artifacts that answer the given problem statement. Because of the complexity issue, the problem design and its solution become crucial for developing an application of the artifact.

3 DESIGN SCIENCE

3.1 Artifacts, research process steps

From theory, we find out that the design science supports a problem-solving paradigm that continually changes the perspective of design processes and artifacts designed to the same difficult problem. The main two processes used in design science iteration for IS artifacts are built and evaluated (Hevner, 2004).

For the three main research questions in this report, the build- evaluate loop in this research was iterated several times, therefor increasing the quality of the design with each iteration based on the required context. More iterations mean more specific integration and relevance for the designed IS artifacts.

Based on the present behavior several actions are needed: First, analyzing the behavior in the research questions, exploring the phenomena, then researching the present truth. Secondly, gaining enough insight about essential requirements, market access and product lifecycle management in market preparation. Generally, the aim of building the artifacts was to focus on the utility of the solution, build it and evaluate it in as many instances as possible. In a good design science, truth and utility are inseparable. Behavior feeds the design, then the design feeds the theory. This enables the identification of the justification/evaluation weakness internal to the artifact as well as the reassessment and refinement of the artifact with each iteration of the loop.

While in the build-evaluate loop, there was a consideration of the evolution of both the design process and its objects. As requirements constantly changed during the research process, it gradually became a creative stepwise approach.

For the purpose of this research report, we follow several recommended steps of a model designed by Hevner (2004), that are to be considered when building utility and validity into the desired artifact.

1. Design an artifact: creation of an innovative, purposeful artifact
2. Problem relevance: description of problem domain
3. Design evaluation: evaluation of the artifact
4. Research contributions: novelty, innovative problem solving
5. Research rigor: several iterations of the build – evaluate loop to ensure consistency
6. Design as a search process: tested the effectiveness of the design
7. Communication of research: technical but also managerial audiences

3.2 Design an artifact: creation of an innovative, purposeful artifact

For each of the three main research questions followed in this report a design was created based on the needed solution. The artifacts design was strongly linked to the question how a complex problem can be solved in a lean way, considering the stakeholders involved in the product lifecycle.

For the first research question:

- How to stay in compliance with regulatory requirements and export controls during the product lifecycle?

The first steps to answer this question were: to understand the Philips VitalHealth products, the essential requirements for their intended purpose and market access, the business needs for different regions and countries, within which standard and regulatory frame technical documentation would need to provide evidence and lastly, how to adapt the product design and development. Moving one step down from the macro-level solution, one has to build and evaluate an IS artifact in order to answer the research question.

The solution design partly has regulatory controls and market access controls for the company’s products. In the previous stages, it was not designed to be the masterplan for product lifecycle management for software products in Philips-VitalHealth, but after several iterations it became more and more relevant while continuously integrating feedback from the involved stakeholders. Therefore, taking into consideration the essential requirements for software design and configuration became very relevant for market access and regulatory approvals by notified bodies across the world.

The artifact itself would fill in the organizational gap in business practice by bridging information together across different departments, from sales, quality and regulatory to product design and development. It proved serving the organization end to end. Furthermore, strategic insights can be offer by the dashboard, therefore integrating cross department information.

Product	Type	Supply Chain	Legal Manufacturer	Status	Product Manager/Owner
ENGAGE	Standard product	Direct to caregroup	Vitalhealth	Live	
QUEST LINK	Standard product	Direct to customer or market	VitalHealth	Live	
COORDINATE	Standard product	Direct to caregroup	VitalHealth	Live	
INSIGHT	Standard product	Direct to caregroup	VitalHealth	Live	

Table 2 : Dashboard product lifecycle management – general product info

In Table 2, you can follow general product information about four software products that Philips-VitalHealth brings the most revenue, from more than 40 products. Engage, Questlink, Coordinate, and Insight. These four products were also presented in the introduction chapter. In addition, the artifact contains several abstract levels, from which one

can zoom in and out of it, depending on the needed detail level. This offers the right level of complexity for different stakeholders to move the process onwards. Only parts of the artifact design were shared, and the table figure depicts the artifact version in the later stages after a few builds and evaluate loop iterations. Some of the boxes were left out blank on purpose in order to keep an adequate level of confidentiality in the process.

	A	K	S	HO
1	Product	General Product Info	Active Countries	Regions
2	ENGAGE			
6	Security			
13	Privacy			
16	Regulatory			
19	Language			
23	Support			
26	Hosting			
29	Software			
32	Hardware			
36	People			
44	Documents			
47	Medical			
50	Risk			

Table 3 : Product lifecycle essential requirements checklist

Considering the complexity of the IS artifacts, the table 3 only depicts a part of the design used for the artifacts themselves after a few iterations. In the previous design, the iteration was considered for only the regulatory aspects and later for the overall requirements configuration list for the software product. This overall configuration list is comprised of the essential requirements. Second research question:

- How to present the regulatory regional information during the product lifecycle to the various stakeholders for medical serving software?

Generally, regulatory information can get extensive, as its enforcement may be specific for each region or country and executed/conducted by different institutional levels such as state governments or regulatory/notified bodies. In order to gain market access when launching a product on an international market, one has to comply with the regulation of that country.

Knowing upfront about the complexity and overlap in compliance, can drive business rational. In most cases complying to country specific regulation, involves lead-times and regulation can dictate the way that products are designed and developed. Including those country specific requirements in the essential requirements a product. A first step on how to display regulatory information was to start the data collection process. As a constant practice, was inquiring the regulatory professionals if there is a database where all the regulations around the world are centralized.

Before Philips acquired VitalHealth, the company had already invested effort into getting compliant on several markets outside the Netherlands, therefore making it possible to already find a database with standards that are specific to software in healthcare. Philips has a quality & regulatory (Q&R) map that could be taken into consideration with regulatory controls based on the Q&R harmonized requirements additional to non-Q&R compliance requirements.

In terms of quality systems, Philips and VitalHealth were not aligned yet, which led to some knowledge and implementation gaps. Assessing the artifacts from both companies gathering the standards was the first step to be conducted. Having a broad understanding on which standards are applicable for software products seemed to be the best primary approach of bundling information and building a filter type approach based on standard reach.

In the case of Philips, which does not have a long history with software in contrast to its history with medical devices and physical products, it was relevant to understand the standards they followed in the QMS procedures and how it linked to quality and regulatory for software. Philips' harmonized Q&R standards, which are all applicable for software, are described in Figure 17. As the US and Europe constitute the main markets for Philips, it is in the company's interest to follow these regions' compliance requirements. Heavy regulation not only appears on regional but also on country specific level, which requires additional information.

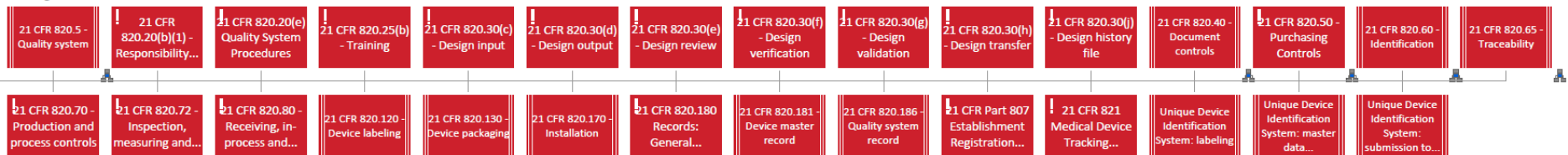
As far as it concerns VitalHealth, the company had experience launching products within the Netherlands and only expanding to few other countries. With the prospect of market expansion, a new artifact had to be built that represented the regulatory standards for specific regions and countries. For example, language requirements can be a bottleneck for market entry. This includes the consideration on what languages the software should entail, and how the built-in languages & labeling can be tendered. Implementing English as user language, makes the product accessible for UK, US, Canada, Australia, India and all other countries that use English in their healthcare act. Including German in software and labeling, the product may be sold in Germany, Austria and Switzerland. Selecting languages therefore may shift the intention of where to sell and where not.

Q&R compliance requirements

(Harmonized) Standards



US Regulations



EU Directives



Country Requirements



EU Directives

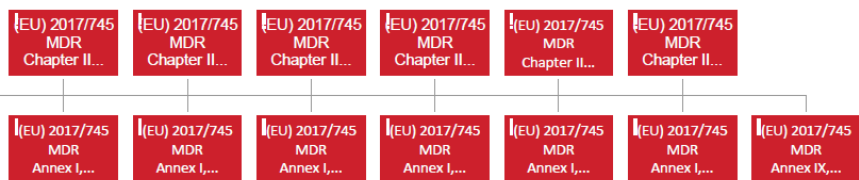


Figure 17 : Phillips Q&R compliance requirements for software



Figure 18: Philips Non-Q&R compliance requirements

Regulation / Norm / Certificate	Title / description	Type	Scope	Area	Relevance	Approach
ISO 27034	Information technology — Security techniques — Application security	Norm	Security	Australia	ISO 27001 add on guideline for application security & life cycle	included in our ISM framework and products, but continuous improvement opportunity needed
ISO 27034	International standard for cyber security: Security Techniques and guidelines for cyber security.	Norm	Security	Australia	ISO 27001 add on guideline for cybersecurity	included in our ISM framework and products, but continuous improvement opportunity for risk management certified
ISO 27001	International standard for information security	Certifiable Norm	Security	Australia	very relevant this the only certifiable security norm; customers ask for this	included in our ISM framework and products
ISO 27002	International standard for information security: Security Techniques and code of practice	Norm	Security	Australia	ISO 27001 implementation guidelines	Incorporate in Platform, Application Development, Application Test and Hosting security checklists. Next to this it will be part of vulnerability and pentests
OWSP top 10	OWSP top 10 2017	Technical norm	Security	Australia	We must comply to this	
ISO/IEC 27017:2015	Information technology -- Security techniques -- Code of practice for information security controls	Certifiable Norm	Security	Australia	Used with ISO/IEC 27001 series of standards, ISO/IEC 27017 provides enhanced controls for cloud service providers and cloud service customers. Unlike many other technology-related standards ISO/IEC 27017 clarifies both party's roles and responsibilities to help make cloud services as safe and secure as the rest of the data included in a certified information management system.	mostly for hosting parties, but interesting for us too
ISO 27018	Information technology - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Certifiable Norm	Security	Australia		mostly for hosting parties, but interesting for us too
ISO 27005	Internationale standaard voor Risk Management op het gebied van informatiebeveiliging.	Norm	Risk management	Australia	best Risk management practice	input for our ISM and QM frameworks
ISO 31000	Internationale standaard: Framework for Risk Management	Norm	Risk management	Australia	best Risk management practice	input for our ISM and QM frameworks
ISO 25010 Product quality	Systems and software engineering - Systems and software Quality Requirements and Evaluation - System and software quality models	Norm	Quality, Product	Australia	relevant for software quality in general	We need a business case and priority for this
ISO 20252	International Standard: Market, opinion and social research — Vocabulary and service requirements	Certifiable Norm	Quality, Product	Australia	This would allow us to offer CQI / PROMS market research services	We need a business case and priority for this
ISO 9001 Quality management systems requirements	International Standard for Quality Managementa.	Certifiable Norm	Quality	Australia	best QA practice	input for our QA framework and processes
ICHOM (International Consortium for Health Outcomes Measurement)	International certificate for standardized measurement results (Value Based Healthcare) in global healthcare.	Certifiable Norm	Product	Australia	good QuestLink certificate; good concepts	Certified
ISO (IEC) 82304 Medical device software - software life cycle processes	International standard: safety and security of health software. Addition to ISO 62304.	Norm	Medical Software	Australia	relevant for CE- marking and medical software development in general	mandatory for Medical Software, best practice for others
MDSAP	Medical Device Single Audit Program	Certifiable Norm	Medical Device	Australia	Very interesting for (near future)	
ISO (IEC) 62366 Medical device usability	International standard: specifies a process for a manufacturer to analyse, specify, develop and evaluate usability of the medical device as it relates to safety.	Norm	Medical Device	Australia	relevant for CE- marking / FDA approval	important for CE-marked products, best practice for others
ISO (IEC) 60601 Medical electrical equipment -: General requirements for basic safety and essential performance	International technical standard for safety and effectiveness of a medical electrical device.	Norm	Medical Device	Australia	relevant for CE- marking / FDA approval	not primary applicable for us as our products are not directly having an electric connection

Table 4 : Representation of standards for Australia for VitalHealth - part 1

Regulation / Norm / Certificate	Title / description	Type	Scope	Area	Relevance	Approach
Continua	Certificated personal connected health device.	Certificate	Medical Device	Australia	Meant for tangible medical devices and their connection to the outside world via PAN/WAN networks	We cannot certify against this and need the specification as long as parties like Philips and Validic deliver us documented API's that we can use for our integrations to them. Next to this many device manufacturers are not Continua certified yet so watchful waiting is also from that point of view ok.
ISO 13485 Medical Devices Quality Management Systems	78/5000 International Standard for Quality Management of Medical Devices.	Certifiable Norm	Medical Device	Australia	relevant for CE- marking / FDA approval	Certified
ISO 14971 Medical devices Application of risk management	International standard for Risk Management in the field of medical devices.	Norm	Medical Device	Australia	relevant for CE- marking / FDA approval	mandatory for CE-marked products, best practice for others
ISO (IEC) 62304 Medical device software - software life cycle processes HL7	International standard for the development of software for medical devices. Health Level Seven: the worldwide standard for secure, electronic information exchange in healthcare.	Norm	Medical Device	Australia	relevant for CE- marking / FDA approval	mandatory for CE-marked products, best practice for others follow
DICOM	Digital Imaging and Communications in Medicine) is a standard that describes how medical image information should be stored, exchanged and printed.	Norm	Integration	Australia	in platform	follow
ISO 27799	International standard for information security in healthcare. Addition to ISO 27002: Guidelines for support and implementation or ISO 27002.	Norm	Imaging	Australia	relevant for international customers	LRQA Audit report available
ISO 14155	Interantional standard with guidelines for conducting clinical patient-related research.	Norm	Healthcare security	Australia	Relevant for clinical trail market and for medical device validation via clinical trials	We cannot certify against this, but use it as input for the clinical trial market; MB to decide on priority
ICH GCP e6	The principles of ICH-GCP were adopted into European legislation, in 2001, with the implementation of the Clinical Trials Directive (Directive 2001/20/EC)	Norm	Clinical Trials	Australia	Relevant for clinical trail market and for medical device validation via clinical trials; harmonized version is useful because it supports FDA regquiremens too	We cannot certify against this, but use it as input for the clinical trial market; MB to decide on priority
GCP WHO	Good Clinical Practice is an international quality standard for clinical trials involving human subjects provided by the WHO	Norm	Clinical Trials	Australia	Relevant for clinical trail market and for medical device validation via clinical trials	We cannot certify against this, but use it as input for the clinical trial market; MB to decide on priority
GAMP 5	Good Automated Manufacturing Practice is a standard with regard to the safety of pharmaceutical products. Provides pragmatic and practical guidelines for secure software.	Norm	Clinical Trials	Australia	Relevant for clinical trail market and for medical device validation via clinical trials	We cannot certify against this, but use it as input for the clinical trial market; MB to decide on priority

Table 5 : Representation of standards for Australia for VitalHealth - part 2

Research question three:

- How to organize the business to ensure delivery of value-added solutions with timely market access?

To answer the third research question based on another iteration of the build-evaluate loop, a second layer of detail was built within the product life cycle masterplan. Mapping the essential steps to undertake the necessary business architecture to fulfill the market access process is the main target of this section. Software configuration, a country and product specific checklist and the constant rechecking and communication with the sales as well as design and development team.

	A	P		A	P
1	Product	Australia	1	Product	Australia
2	ENGAGE		27	Software Add-on	No
3	Security certification	ISO 27001	28		
4	Security legislation	Cybersecurity Act 2001	29	Software	
5	Security Pentesting in Bangalore	Agreed	30	Devices	Gluco meter Weighting scale Blood Pressure
6	Security		31	Compatibility	Yes
7	Privacy new	The Privacy Act 1988 (2018 version)	32	Hardware	
8	Privacy	The Privacy Act 1988	33	Project lead launch Market	Confidential
9	Privacy Officer	Required	34	Project lead launch Market VitalHealth	Confidential
10	Privacy Impact Assessment	Required	35	Regulatory contact /sponsor	Sponsor required
11	Supervisory Authority	Office of the Australian	36	People	
12	Compliant (Yes/No)	Yes	37	Documents - Country QMS	ISO 9001
13	Privacy		38	Required documents	Australian Declaration of Certificate of Inclusion
14	Regulatory Registration	TGA Registration	39		Essential Principles Checklist
15	Regulatory sponsor	Local	40		Regulatory Plan
16	Regulatory		41		Assessment of TechNology.
17	Default Language	English	42	Inter company Quality agreement	Required
18	Optional Language	None	43		
19	Language		44	Documents	
20	1th line Support	Philips Australia?	45	Disease	diabetes, Heart failure, oncology
21	2nd line Support	VitalHealth India?	46	Medical	
22	Complaint handling	Service max, One EMS, Trackwise	47	Risk	low
23	Support		48	Risk/Benefit	TBD
24	Hosting on Premise	Australia AWS or on premise	49	Risk	
25	Hosting in Cloud, Open Link, Azure Microsoft	Microsoft	50		

Table 6 : Essential requirements checklist - Engage

3.3 Problem relevance: description of problem domain

In the process of developing and building an IS artifact, the problem relevance is dictated by the business needs. In the case of Philips VitalHealth, checking for the utility of the constructed IS artifacts was a constant practice and varied in process.

To better understand the Environment, which is defined into IS research, three dimensions have to be considered according to Hevner (2004): People, Organizations, Technology (see Figure 19).

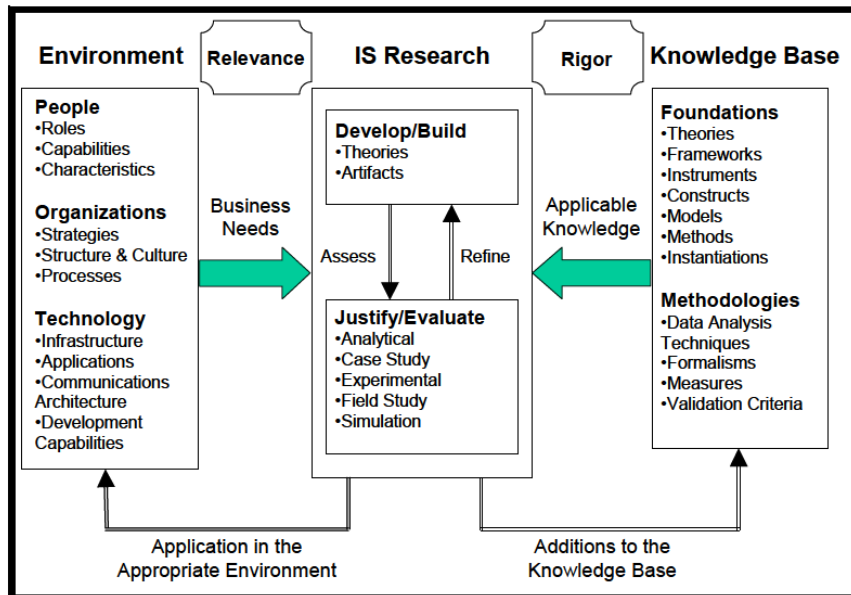


Figure 19 : IS research framework

People: Weekly meetings and interviews were conducted to better understand how people worked within the organization and build relevance for their roles based on the process they had to fulfill.

Organization: There was relevance to build utility within the organization between Q&R and product development. Interviews were conducted with the head of Q&R and product owners. Product development on the other hand talked about the essential requirements, the change control procedure and the harmonized standards applied. In addition to the internal relevance, there was also an external validation point from a consultant that had experience with notified bodies, where the audit needed to be prepared.

Based on the interviews and the assessment done on the present artifacts, Philips VitalHealth agreed together with the Head of Quality & Regulatory to only pursue the bare minimum standards to be compliant. It was decided to choose another design for presenting the regulatory information. It was now possible to filter for specific country regulations and harmonized standards as you can see in the example for Belgium in table 7. Additionally, a plot was created to show a lean based regulatory requirement availability.

Regulation / Norm / Certificate	Title / description	Type	Scope	Area	Relevance	Approach
Act of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as amended by the Act of 11 December 1998 (the Data Protection Act)	This act aims to protect individuals against abuse of their personal data. The rights and obligations of the individuals whose data are processed, as well as the rights and obligations of those processing the data have been established by the Privacy Act.	Regulation	Privacy	Belgium		
Royal Decree of 13 February 2001	Contains further implementing provisions of the Data Protection Act	Regulation	Privacy	Belgium		
ISO 27034	Information technology – Security techniques – Application security	Norm	Security	Belgium	ISO 27001 add on guideline for application security & life cycle	included in our ISM framework and products, but continuous improvement opportunity needed
ISO 27034	International standard for cyber security: Security Techniques and guidelines for cyber security.	Norm	Security	Belgium	ISO 27001 add on guideline for cybersecurity	included in our ISM framework and products, but continuous improvement opportunity for risk management
ISO 27001	International standard for information security	Certifiable Norm	Security	Belgium	very relevant this the only certifiable security norm; customers ask for this	certified
OWSP top 10	OWSP top 10 2017	Technical norm	Security	Belgium	We must comply to this	Incorporate in Platform, Application Development, Application Test and Hosting security checklists. Next to this it will be part of vulnerability and pentests
ISO (IEC) 62366 Medical device usability	International standard: specifies a process for a manufacturer to analyse, specify, develop and evaluate usability of the medical device as it relates to safety.	Norm	Medical Device	Belgium	relevant for CE- marking / FDA approval	important for CE-marked products, best practice for others
ISO 13485 Medical Devices Quality Management Systems	78/5000 International Standard for Quality Management of Medical Devices.	Certifiable Norm	Medical Device	Belgium	relevant for CE- marking / FDA approval	Certified
ISO 14971 Medical devices Application of risk management	International standard for Risk Management in the field of medical devices.	Norm	Medical Device	Belgium	relevant for CE- marking / FDA approval	mandatory for CE-marked products, best practice for others
ISO (IEC) 62304 Medical device software - software life cycle processes	International standard for the development of software for medical devices.	Norm	Medical Device	Belgium	relevant for CE- marking / FDA approval	mandatory for CE-marked products, best practice for others
ISO 27799	International standard for information security in healthcare. Addition to ISO 27002: Guidelines for support and implementation or ISO 27002.	Norm	Healthcare security	Belgium	relevant for international customers	LRQA Audit report available
GDPR	General Data Protection Regulation, AVG (Algemene verordening gegevensbescherming)	Regulation	Privacy	Belgium	not effective yet, but will replace WBP and have big impact	We comply procedurally and technically for most products
MDR	Medical Device Regulation	Regulation	Medical Device	Belgium	relevant for CE- marking	mandatory for CE-marked products, best practice for others
CE - marking	A manufacturer's declaration that the product complies with the essential requirements of the relevant European health, safety and environmental protection legislation.	Certifiable Norm	Medical Device	Belgium	relevant for Mentalhealth screener	CHM, Insight, QM and e-Vita are certified class I

Table 7 : Regulations harmonized standards table for Australia

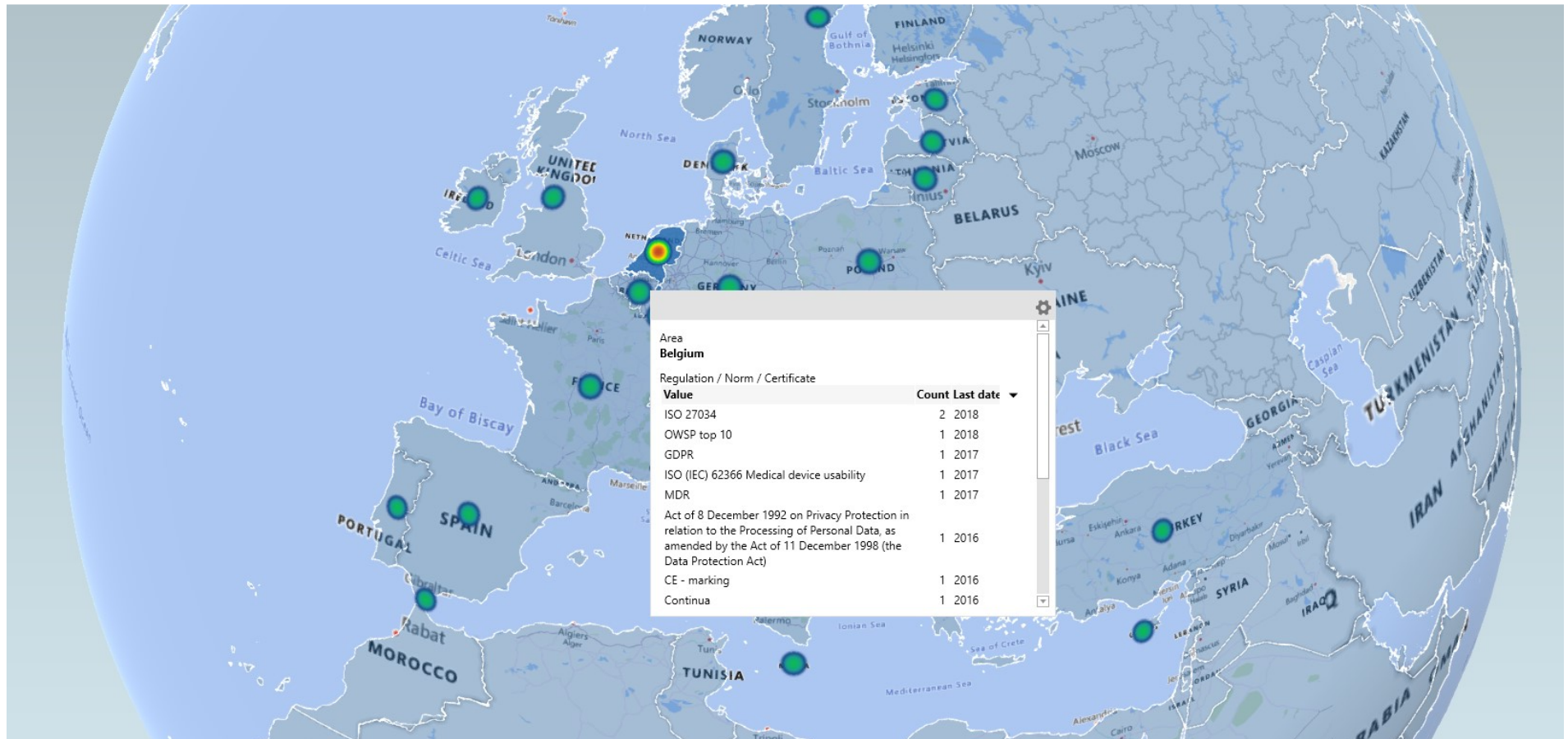


Figure 20 : Global compliance heat map of harmonized standards - Belgium

3.4 Design evaluation: evaluation of the artifact

Table 2. Design Evaluation Methods	
1. Observational	Case Study: Study artifact in depth in business environment
	Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study fit of artifact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability)
	Simulation – Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Figure 21 : Design science evaluation methods table

The design evaluation for the Philips VitalHealth product lifecycle masterplan, and regulatory action-based design followed all the methods that Hevner (2004) used in his design science approach, mainly because the artifact needed to be evaluated in terms of functionality.

After a few iterations, data consistency, process accuracy and completeness were reached. Methodically, I chose four out of five methods (Hevner, 2004): observational, analytical, testing and descriptive.

Additionally, information reliability and usability were tested. To better explain the aim of using these methods was to have the evaluation loop, that built up the relevant inputs for reconstruction in several iterations.

The observational case study was used as a method, by studying the behavior of the artefact in business environment at the conjunction of Q&R, product development and sales.

In interviews with the Q&R and Sales a static analysis was conducted examining the complexity needed around the required knowledge. In addition, several iterations were performed on the artifact to ensure optimization of the desired behavior: For the export control part, three artefacts that were previously used were now integrated into one dashboard with the support of Q&R and commercial control.

Based on input from the external consultant with a notified body perspective, Q&R acquired knowledge on business practice, building arguments to prove the utility of changing the internal business process in order to comply with different audits.

3.5 Research contributions: novelty, innovative problem solving

One of the unsolved problems was regulatory and export control while in the development process, that could either stall or stop the overall process in sales and product development.

According to design science, the artifact must represent a reality and should be implementable (Hevner, 2004). At the beginning of the research, there was no specific artifact, that could generate the overview about market access and regulatory control. The then needed meeting and call to push for activity introduced a lag in the overall process. Again, I started a data gathering process at the conjunction between Q&R and export control.

For each of the products there are different regulatory processes and intercountry agreements that need to be taken into consideration: i.e. in Iran shipment is not allowed, whereas if the risk-benefit analysis proved positive for Austria, the export and regulatory control would put the activity IP. Given the scope and behavior needed, each product contained a different risk profile.

	A	K	L	M	N	O	P	Q	R
Product	General Product Info	USA	Austria	Belgium	Saudi Arabia	Australia	China	Singapore	
ENGAGE		IP	N	IP	IP	IP	IP	IP	
QUEST LINK		Y	IP	Y	IP	IP	IP	IP	
COORDINATE		N	N	N	N	N	N	N	
INSIGHT		N	N	N	N	N	N	N	

Table 8 : Product - global approbation matrix - market access

Legend for Approval Status	
Y	Shipment allowed
N	Shipment not allowed
IP	Approbation activities: In Process. Shipment not allowed
N	Shipment not allowed due to trade restrictions, or Export license

Table 9 : Approval status legend

3.6 Research rigor: preparations for the build – evaluate loop

Choosing several businesses that had previously been in the same spot as Philips VitalHealth accounts for research rigor.

Having knowledge on what standards to build compliance first helps in generating a winning strategy with the least costs involved. The decision of certifying first against EU regulation, harmonized standards and the US market, supports gaining competitive advantage. An external consultant with international expertise was employed and used for referencing to theories and business practices while the Q&R team underwent training.

In those trainings the Q&R team was involved and trained in such a way that the team could scale the provided training for the whole organization. The training were to be designed in such a way that they would build up a critical mass of people that can lead the change of a controlled practice in market access and product development.

There was utility in having such a dashboard with the overview over the product lifecycle management, with the rigor of a previous proven development based on point of view of notified bodies.

In the case of Australia, one can only present products to potential customer, once the product has been proved compliant with the Australian market. It was therefore necessary to figure out which was the fastest way to get compliant to the Australian market and how to reach a protocol with the Australian healthcare provider. This required the acquisition of knowledge about the certification process.



Australia

Time, Cost, and Complexity of Registration

Device classification in Australia	Class I Non-sterile; Non-Measuring	Class I Sterile or Measuring	Class IIa	Class IIb	Class III
How long you should expect to wait after submission until approval is granted. ¹	<1 month	2-3 months	2-3 months	2-3 months	7-14 months
Validity period for device registrations/ ARTG listing. ²	Does not expire	Does not expire	Does not expire	Does not expire	Does not expire
Registration renewal should be started this far in advance. ³	1 month	1 month	1 month	1 month	1 month
Complexity of the registration process for this classification. ⁴	Simple — Complex ●————○	Simple — Complex ●————○	Simple — Complex ●————○	Simple — Complex ●————○	Simple — Complex ●————○
Overall cost of gaining regulatory approval. ⁵	Low — High ●————○	Low — High ●————○	Low — High ●————○	Low — High ●————○	Low — High ●————○

Figure 22 : Australian regulatory roadmap for medical devices

After gaining knowledge about the harmonized standards in the Australian regulation, the regulatory team started to work with product development to have the registration process in place. As you can see in Figure 22, Australia has a different classification system compared to the Europe and US, henceforth the study of the regulation is a timely and thorough process. The utility of having control over this aspect in a development process becomes mandatory.

3.7 Design as a search process: effectiveness of the design - Iterations

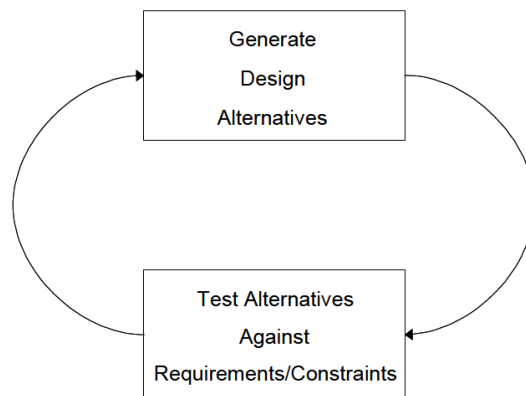


Figure 23 : Build evaluate loop

Design science is inherently iterative. The research questions were inherently answered by having several iterations including knowledge base efforts, previously used artifacts and interviewing the relevant stakeholders. Putting effort into several iterations based on interest, relevance, optimization and utility resulted in a more effective solution.

3.8 Communication of research: technical but also managerial audiences

A challenging aspect was how to communicate the rather complex solution to different audiences. It proved suitable to create two layers of complexity within the masterplan for product lifecycle management. Based on the department to be addressed its purpose was communicated in different manners. The first level of complexity presents a high-level abstract with control measures used on managerial level, in Q&R and Sales. The second layer of complexity serves as a source for each product's essential requirements whereas the design team acknowledges the requirements and decide for a plan to deal with them, in most of the cases elements from the essential requirements checklist become part of the product documentation and serve the intended technical audience.

The design aims to develop innovative solutions, which define ideas, practices, technical capacities, and products, that can effectively and efficiently stimulate critical thinking in analyzing, designing, implementation, managing and using information systems. However, design of useful artifacts is complex among IS practitioners, because there is need for creative progress in fields where current theory is often not adequate.

Having both audiences in mind, the top down and bottom up approach can funnel congruent efforts and build up to a successful implementation of requirements into the software.

4 CONCLUSIONS

For the conclusions chapter let us reconsider the research questions.

- How to stay in compliance with regulatory requirements and export controls during the product lifecycle for medical software?
- How to present the regulatory regional information during the product lifecycle to the various stakeholders?
- How to organize the business to ensure delivery of value-added solutions with timely market access?

Most attention was paid to the first and second research question. The data needed to stay compliant was collected and presented by means of an IS artefact to the stakeholders. Using the design science approach relevance and utility was built into the IS artefact which made it to a masterplan for product lifecycle management.

The third research question is one that has to be answered in daily practice. However, it is clear that not complying to the required processes for safety critical software can have serious consequences, as has been experienced by Philips in the past and Boeing as we speak.

Presenting all the regulatory information in an actionable way is a necessity to put it to use by business and engineering people within a company. The regulatory information has to be communicated and adapted for different audiences both managerial and technical. The recommended action is to treat certain regulatory aspects by design. Identifying the key harmonized standards for software in healthcare and having a clear view in the early stages on how to stay compliant becomes a winning strategy. For software in healthcare it is imperative to treat security and privacy by design, safeguarding patient's data.

Having a set of harmonized standards on which the product is minimum compliant, makes the process of gaining approval from the country notified body faster. The process of gaining market access is more rapid because of less design & development time and more quality already built in the software products. Including harmonized standards for each of the products builds up a more robust portfolio of products. Therefore, applications towards the notified body can be submitted for a family of products not only for individual products. If applications are sent for a family of products the cost is depending on the countries specific requirements but in most cases is decreased drastically.

Quality and regulatory, must have a role and be in control at key milestones in development a release of a safety critical software product. Therefore, making a regulatory plan and an actionable dashboard where all the above-mentioned controls such as configuration control, change control, regulatory control, export control, are displayed is certainly relevant from the product lifecycle perspective.

5 LIMITATIONS & FUTURE RESEARCH

There were 3 major limitations identified when doing the design science research report. All of them serve as a basis for future research. Design science offers an extensive level of freedom by its method approach. In the design & implementation of IS artefacts various technologies can be used to achieve effectiveness between stakeholders.

The environment conditioned a technology limitation while doing the research. VitalHealth was acquired by Philips at the end of 2017. When this research report was in the final stage, the company was in the middle of the transition period between the IS systems. VitalHealth already had been using own procedures and IS Systems that made them successful in the past, but they were undergoing internal changes to adapt to the Philips practices. At the moment when VitalHealth had to choose the type of tooling to construct the masterplan for product lifecycle management, Power BI and SAP were considered. In the end the tooling was not available due to delays in transitional changes which led to the choice of building the design for regulatory control and market access in excel instead.

This research helped with the initial design and implementation of the IS artefact and serves for the future transition to SAP systems. The SAP system can provide an automated version of the same design rationale. An interesting aspect to follow by future research will be the transition to SAP automating market access, regulatory control, and change control.

The second limitation comes from the lack of possibility to observe the IS artifact in the actual field. Future research can focus on monitoring the behavior of the IS artefact in multiple projects.

The third limitation was given by the lack of functional and structural testing, from a black box and white box perspective. It would be interesting to see if the interface used in the design is intuitive enough or whether training needs to be done to implement it. Ultimately, the structural test would be an interesting aspect to follow, based on the implementation and the paths it provides by syncing Q&R with Product Development and Sales.

6 BIBLIOGRAPHY

European commission (2017), ISA2, The new Interoperability framework. Retrieved in 25.1.2019 from <https://ec.europa.eu/isa2/sites/isa/files/docs/publications/eifa4.pdf>

European Commission. (2018). Regulatory framework - European Commission.

Eysenbach, G. (2001). Evidence-based Patient Choice and Consumer health informatics in the Internet age. *J Med Internet Res*.

FDA (2019). Medtronic, Inc. Recalls Dual Chamber Implantable Pulse Generators (IPGs) Due to Possible Circuit Error. Retrieved in 01.6.2019 from <https://www.fda.gov/medical-devices/medical-device-recalls/medtronic-inc-recalls-dual-chamber-implantable-pulse-generators-ipgs-due-possible-circuit-error>

Fuentes M.R & Huq N (2018), Securing Connected Hospitals A Research on Exposed Medical Systems and Supply Chain Risks, MicroTrends Publication.

Handayani, P. W., Rahman, M. Z., & Hidayanto, A. N. (2013). Information technology assessment on hospital information system implementation: Case study a teaching hospital. *International Journal of Engineering and Technology*, 5(2), 631-634.

Hatton Les, Rutkowski, Anne (2019). “Lessons Must Be Learned”—But Are They? *IEEE Software*, July/August 2019.

Hevner et al. (2004). Design Science in IS Research. *MIS Quarterly*, Vol.28(1), 75-105.

Holzmann, G. J. (2013). Landing a spacecraft on mars. *IEEE Software*. <https://doi.org/10.1109/MS.2013.32>

Joyce M. S. França, J. d. (2017). Development of an Electronic Health Record Application using a Multiple View Service Oriented Architecture. Proceedings of the 19th International Conference on Enterprise Information Systems, 308-315.

Kolodner, R. C. (2008). Health information technology: strategic initiatives, real progress. *Health Affairs*, Vol. 27, 391–395.

Massdevice (2019). FDA gives massive Medtronic recall Class I designation. Retrieved in 01.6.2019 from <https://www.massdevice.com/fda-gives-massive-medtronic-recall-class-i-designation/>

Medtronic (2019). Dual Chamber Pacemakers: Urgent Medical Device Recall | Medtronic. Retrieved in 01.6.2019 from <https://www.medtronic.com/us-en/healthcare-professionals/products/product-performance/dual-chamber-pacemaker-recall.html>

Middleton, B. S. (2016). Clinical decision support: a 25 year retrospective and a 25 year vision. *IMIA Yearbook*.

Mayer N, Aubert J., Grandry E., Feltus, Goettelmann E., Wieringa R. (2018). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software and System Modeling*. pp 1-28.

Mucheleka, M., & Halonen, R. (2015). ERP in Healthcare. In *ICEIS (1)*. pp. 162-171.

- Philips (2018). News Press Room Philips Retrieved in 1.06.2019 from <https://www.philips.com/a-w/about/news/archive/standard/news/press/2018/20181102-philips-to-open-new-center-of-excellence-for-diagnostic-imaging-r-and-d-in-cleveland.html>
- Radley, D. W. (2013). Reduction in medication errors in hospitals due to adoption of computerized provider order entry systems. *J. Am. Med. Inform. Association*.
- Rossiter, S., Noble, J., & Bell, K. R. (2010). Social simulations: Improving interdisciplinary understanding of scientific positioning and validity. *Journal of Artificial Societies and Social Simulation*, 13(1).
- Rutkowski A., M. van Genuchten and L. Hatton, (2018) "No Free Lunch for Software after All," in *IEEE Software*, vol. 34, no. 5, pp. 13-15.
- Midha, Vishal & Ngafeeson, Madison & Ghosh, Kaushik. (2017). Healthcare IT: Current Research and Future Trends. *International Journal of Electronic Healthcare*. 9. 89-99.
- Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., ... Yaseen, A. (2017). Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2017.2767561>
- TÜV SÜD (2018). TÜV SÜD - Medical Device Regulation (MDR) | TÜV SÜD <https://www.tuvsud.com/en/industries/healthcare-and-medical-devices/medical-devices-and-ivd/medical-device-market-approval-and-certification/medical-device-regulation>
- VitalHealth (2019). eHealth Solutions - VitalHealth Software. Retrieved in 1.06.2019 from <https://www.vitalhealthsoftware.com/>
- Zarsky, T. Z. (2016). Incompatible: The GDPR in the Age of Big Data. *Seton Hall L. Rev.*, 47, 995.