Becoming a Medical Device Software Supplier and Complying with Data Security Regulations

Fergal McCaffery, Ronald Jabangwe, Kitija Trektere,
Regulated Software Research Centre & Lero,
Dundalk Institute of Technology
Dundalk, Co.Louth, Ireland
e-mail: {fergal.mccaffery, ronald.jabangwe, kitija.trektere }@dkit.ie

Garret Coady
BlueBridge Technologies
3015 Lake Drive, Citywest, Dublin 24, Ireland
e-mail: {garretcoady}@bluebridgetech.com

***Abstract*—Today many software development companies are restructuring their business model to enter the medical device domain. The reason for this change is that significant opportunities exist within the healthcare industry and particularly in relation to the usage of software within this domain. However, in order to become either a medical device software supplier or manufacturer there are challenges to overcome, and data protection regulations to abide by. This paper describes a case study of an Irish software development company that in 2014 decided to change their business model to enable them to become a medical device software supplier, and engaging with clients in the United States of America. The paper provides an account of their journey from being an automotive software supplier to securing software development contracts from leading medical device manufacturers. This involved them having to re-design and re-structure their software development approach to meet both the demands of medical device standards, data security regulations and medical device multinational third party software selection criteria.**

Keywords-MDevSPICE® Framework; Software Development Process; Medical Device Software; Software Security; HIPAA; Agile Software Development.

I. Introduction

The enormous and seemingly ever-growing medical device market value motivated the case company presented in this paper to shift to a medical device software supplier [1]. In 2015, the medical device (MD) global market was "valued at \$228 billion, up from \$164 in 2010 and projected to reach \$440 billion by 2018" "at approximately 4.4% compound annual growth rate per year" [2]. The leaders in the MD market are the United States of America (USA) having 38% of the global value of this market followed by China with a market valued at \$48 billion with western Europe having almost 25% of the global market [2]. However, to become a MD supplier for the industry takes significant time and resources as there are many obstacles that need to be overcome.

This paper extends the paper presented in [1], which is based on a case study of an Irish software development company *BlueBridge Technologies* (BBT). Their journey started in 2014 when BBT decided to embark upon becoming a MD software supplier and at that moment they had no regulatory requirements in place, in fact a key question they asked at that stage was *"what are the standards we need to implement and in what order?"*. This paper presents how with the help of academic MD researchers' regulations were put in place through undergoing an MDevSPICE® assessment and outlining the challenges that might arise in the near future.

The rest of this paper is organized as follows. Section II describes the background of BBT and the current situation in the MD industry. Section III outlines the challenges BBT faced in order to become a MD software supplier. Section IV describes the approaches followed to become a MD software supplier. Section V outlines given that BBT have satisfied the regulations they wish to further refine and improve their software development processes to make them more efficient. Section VI describes first steps taken in order to improve their current lifecycle process and approach to ensuring data security. Recommendations to the case company are provided in Section VII. The final section of the paper provides a conclusion and future work in Section VIII.

II. Background of the Company

BBT was founded in 2006 – initially formed upon the closure of the Irish based development operations of Magna Automotive, and today employs 19 people with 8 of them working as software developers. BBT are currently working on 7 different projects with 5 of them involving developing the software component for another organization's product. Their current customers include pharmaceutical and multinational MD companies.

The main reason why software development companies wish to enter the MD domain is because of the expansion of the MD industry in the past few years therefore providing many opportunities for others to enter into this industry. The MD industry is largely research and development driven.

Software increasingly performs an essential role in the provision of healthcare services [3]. This is particularly reflected in the importance that software now plays in medical diagnoses and treatment [4]. The level of software functionality in MDs and the complexity of that software has substantially increased [5]. The MD regulatory environment has been extended to include more focus on software. For example, the latest amendment to the Medical

Device Directive [6] recognizes that standalone software can be classified as a MD in its own right. Consequently, a significantly increased proportion of software applications will now be classified as MDs and must be developed in a regulatory compliant manner [7].

Medical records are increasingly being stored in electronic form. The use of Electronic Medical Record (EMR) systems in the USA by physicians increased from 18.2% in 2001 to 48.3% in 2010 [8]. The adoption of EMR systems could produce efficiency and safety savings of $81 billion annually and improve prevention of medical diseases [9]. Use of Mobile devices in health care is increasing. “By 2017, mobile technology will be a key enabler of healthcare delivery reaching every corner of the globe” [10].

III. Challenges BBT Needed to Overcome to Become a MD Software Supplier

To become a MD software supplier there were regulations and standards that needed to be adhered to. This required processes to be defined in accordance with these standards and regulations and then for objective evidence to be obtained demonstrating the implementation of the defined processes. For BBT, the starting point was to gain an understanding of three main standards and data protection regulations in the US. The paragraph below briefly outlines the standards that BBT familiarized themselves with before starting to define their MD software development processes.

A. ISO 13485:2006

“This International Standard specifies requirements for a quality management system that can be used by an organization for the design and development, production, installation and servicing of medical devices, and the design, development, and provision of related services” [11].

ISO 13485 is in practice required by any MD company. It details the requirements for the Quality Management System (QMS) for MDs. The standard is broadly based on ISO 9001, although the 2015 revision of the latter departs significantly from the previous approach. ISO 13485 was recently revised in 2016, resulting in a better alignment with the Food and Drug Administration (FDA) regulations; changes include explicit requirements for validation of software infrastructures used by the company.

ISO 13485 is a “Harmonized Standard” for the EU and a “General Consensus Standard” for the FDA.

Certification to ISO 13485 is achieved by independent audit by a Notified Body of the Quality System of the company. It involves yearly surveillance audits and re-certification every 3 years.

B. IEC 62304

“This standard defines the life cycle requirements for MEDICAL DEVICE SOFTWARE. The set of PROCESSES, ACTIVITIES, and TASKS described in this standard establishes a common framework for MEDICAL DEVICE SOFTWARE life cycle PROCESSES” [11].

IEC 62304 covers the development process for medical device software. This standard is harmonised with the requirements of ISO 13485 and therefore complements it by adding the specifics required for MD software.

Similarly to ISO 13485, IEC 62304 is a “Harmonized Standard” for the EU and a “General Consensus Standard” for the FDA.

However, IEC 62304 interfaces with ISO 13485 in two areas: software inputs and system integration. The software inputs are generated from the system (or subsystem) level requirements, while IEC 62304 explicitly does not cover system level activities, in particular design validation.

Although this is the gold standard for the development of MD software, there is no such thing as accreditation or certification to IEC 62304. Anyway company can request an “independent certification” by a Notified Body and this is particularly attractive to MD software suppliers.

C. ISO 14971:2009

“This International Standard was developed specifically for medical device/system manufacturers using established principles of risk management. For other manufacturers, e.g., in other healthcare industries, this International Standard could be used as informative guidance in developing and maintaining a risk management system and process”[13]. “This International Standard deals with processes for managing risks, primarily to the patient, but also to the operator, other persons, other equipment and the environment” [13].

ISO 14971 is particularly important to any MD manufacturer and supplier. Most decisions made during the whole lifecycle of a device must be risk-based.

The area of regulatory standards and the recording of documentation associated with their implementation was new to BBT. Therefore, BBT engaged with both standards consultants and an academic research group (the RSRC, our research centre) specializing in MD software development research. This assisted BBT to fast-track the initial steps to becoming a MD software supplier.

D. Data Security Regulations: Protecting Health Information

In the US, the law that outlines and standardizes the protection of health information is HIPAA (Health Insurance Portability and Accountability Act) [29]. HIPAA refers to health information as protected health information (PHI) or electronic protected health information (EPHI).

PHI or EPHI includes health information and any accompanying information that can be used to identify an individual, such as, demographical information, that is created, stored, transmitted or maintained when providing health-related services [30].

HIPAA mainly consists of four Rules that state what and how data should be protected, which are [29]: the Privacy Rule, Enforcement Rule and the Breach Notification Rule, Security Rule. The Privacy Rule outlines the standard expected for the protection of personal health or medical information. In the event of violations, for example, inappropriately protecting PHI, the provisions on penalties and related procedures are outlined in the Enforcement Rule. Provisions for the required course of action in case of any breach on protected health information is outlined in the Breach Notification Rule. The Security Rule outlines safeguards that are needed to secure EPHI/PHI that is either created, stored or transmitted.

IV. Approach to Become a MD Software Company

When BBT reached out to the RSRC, we knew that this was an ideal company to become involved with in regards to performing research into how software companies could make the transition to becoming MD software suppliers.

A. Embark on MDevSpice® assessment

First of all, it was essential to understand BBT's current position in regards to their software development processes. We decided to perform an MDevSPICE® [14] assessment. MDevSPICE® is a framework assessment model where all MD software standards and processes are brought together into one place with software engineering best practices. MDevSPICE® was developed in the RSRC. Then, this framework assessment model was utilized in BBT to assess the current situation.

Below we describe what happened next in regards to both the assessment and BBT's subsequent journey to becoming a MD software supplier.

A) Assessment conducted: Given that MDevSPICE® consists of 23 processes we selected the most appropriate 10 processes from the MDevSPICE® model to assess BBT against (see Table I).

It was agreed upon discussion with BBT that only the most foundational processes would be assessed. Therefore, the following 10 out of the 23 MDevSPICE® processes were chosen to be assessed over 2 onsite days in BBT.

The order of the processes assessed was important as it is important to follow the medical device software development lifecycle. Therefore, systems requirements were a very natural place to start. Below is outlined the process assessment schedule: we assessed 5 processes on each day (see Table II).

Each process was assessed by 2 MDevSPICE® assessors in an interview with at least 2 members of BBT being present in each interview. Prior to the interviews both the schedule and the names of the BBT staff members that would be involved in each process interview was agreed. It was very important to ensure that access was provided to the most relevant staff for each interview session as otherwise the assessment would not have been as accurate as possible.

TABLE I. PROCESSES OF MDEVSPICE®

MD System Lifecycle Processes	*MD Software Lifecycle Processes*	*MD Support Processes*
Project Planning Project Assessment and Control Risk Mgmt. Stakeholder Req. Definition System Req. Analysis System Architectural Design System Integration System Qualification Testing Software Installation Software Acceptance Support	Software Dev. Planning Software Req. Analysis Software Architectural Design Software Detailed Design Software Unit Implementation. and Verification Software Integration and Integration Testing Software System Testing Software Risk Mgmt.	Configuration Management Software Release Software Problem Resolution Software Change Request Management Software Maintenance

TABLE II. DAY 1 AND DAY 2 OF ASSESSMENT PROCESS

Onsite Assessment Day 1
System Requirements Analysis
Software Development Planning
Software Requirements Analysis
Software Architectural Design
Software Detailed Design
Onsite Assessment Day 2
Software Unit Implementation & Verification
Software Integration & Integration Testing
Software System Testing
Software Risk Management
Software Configuration Management

Each of the 10 interviews lasted approximately 1 hour and involved one assessor asking BBT staff a set of scripted questions related to that process area. The second assessor used a tool to record detailed responses from the interviewees with both assessors using the tool to enable each question to be scored as "Fully Achieved", "Partially Achieved" or "Not Achieved". In addition to the usage of predefined scripted questions additional questions were also asked that were specific to BBT.

B) Findings produced: The MDevSPICE® assessors at the end of Day 2 returned back to the RSRC and went through each process together, discusssing the observations and notes from the assessment. As a result of performing the assessment we provided BBT with a set of strengths, issues and recommendations to address those issues across each of the assessed processes. The MDevSPICE® assessment provided coverage over a number of different MD software related standards. Figure 1 shows a breakdown of the coverage provided for each of the different standards from assessing 10 of the 23 MDevSPICE® processes. As one of the goals of BBT Management was to gain an understanding in relation to the state of their current development processes against IEC 62304, as this is the main MD software process standard, processes were selected from MDevSPICE® that featured heavily in IEC 62304. The exception to this was System Requirements Analysis but this was deemed to be a critical process to examine as BBT would be performing software development for an overall MD system. Therefore, it is essential that they have an efficient process in place for System Requirements Analysis as otherwise everything that occurs afterwards within the development lifecycle will be impacted.

From looking at Figure 1 it can be seen that the 10 processes assessed provided: 59% coverage of IEC 62304; 2% of ISO 80002-1 [15] (this technical report relates to how ISO 14971 may be applied within software); 16% of the FDA's Guidance for off the shelf software [16]; 1% of the FDA's Guidance for premarket submissions [17]; 20% of the FDA's Guidance for validation of software [18]; 1% of ISO 13485 and 1% of software engineering best practice standards.

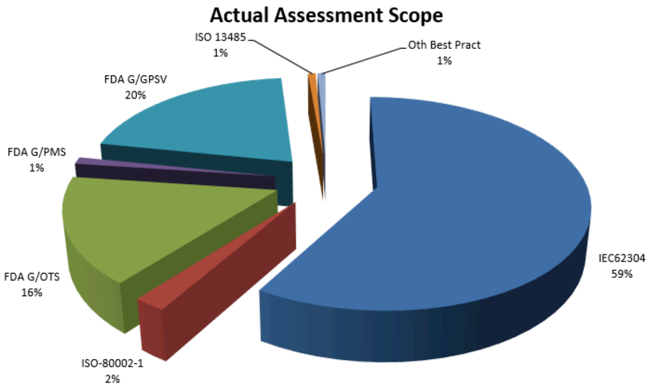


Figure 1. Scope of the BBT Assessment

C) Implementing the recommendations: In order to assist BBT to implement the recommendations in a timely manner BBT took the following steps:

a) Brought in consultants to assist with the implementation of QMS 13485.

b) Recruited an engineer from a leading MD manufacturer who possessed considerable experience in developing MD software development and in particular MD risk management expertise to put in place a risk management strategy in line with ISO 14971.

c) Engaged with a notified body organisation to prepare them for an official audit in IEC 62304 and subsequently perform the audit. This enabled an successful IEC 62304 audit to be achieved in a timely manner.

D) Actions taken by BBT:

a) Gained Certification to ISO 13485

b) Gained Independent Certification in IEC 62304.

c) The IEC 62304 audit was performed against one project using a plan driven approach.

d) BBT have the MD standards that MDs maufacturers request software suppliers to have in place.

The main criteria MD manufacturers use for selecting a MD software supplier is that organizations should have IEC 62304 in place. At this stage BBT now have not only satisfied this criteria but surpassed it in that they not only adopted IEC 62304 but were certified against it and also have adopted IEC 13485, ISO 14971, 21 CFR 820 and the FDA Guidance documentation for: Off the shelf software, Premarket Submissions and Validation of MD software. Therefore, at this stage BBT were ready to obtain contracts as a MD software supplier company.

E) Addressing HIPAA Safeguards

We are currently working with BBT to ensure that their software meets HIPAA requirements. In order to so, we are using the international medical device security technical report IEC/TR 80001-2-8 [31] to identify security controls that can be implemented in order to address the HIPAA safeguards.

IEC/TR 80001-2-8 provides a guidance "for the selection and implementation of management, operational, administrative and technical security controls to protect the confidentiality, integrity, availability and accountability of data and systems during development, operation and disposal." [31].

IEC/TR 80001-2-8 extends another security standard IEC/TR 80001-2-2 [32], which lists 19 security capabilities that are needed to ensure data security. IEC/TR 80001-2-8 extends IEC/TR 80001-2-2 by outlining a list of security controls for each of the security capabilities. The capabilities are broad and range from technical capabilities, e.g., "Automatic logoff" [31,32], to those that can be traced to documentation or policies, e.g., "Security guides" [31,32].

The mapping of security controls to security capabilities in IEC/TR 80001-2-8 is based on an extensive review of security controls outlined in the following security related standards and guidelines: NIST SP 800-53 (Revision 4) [33], ISO/IEC 15408-2:2008 [34], ISO/IEC 15408-3:2008 [35], IEC 62443-3-3:2013 [36] and ISO IEC 27002:2013 [37].

IEC/TR 80001-2-8 can be used to support the decision-making process when selecting security controls in order to achieve security capabilities for medical device software. The standard aims to help companies with identifying and implementing appropriate security controls to help "protect the confidentiality, integrity, availability and accountability of data and systems during development, operation and disposal." [31].

V. CURRENT STATUS OF THE CASE COMPANY: LESSONS AND CHALLENGES

First, once BBT became a MD software supplier they noticed the significant attention within the MD field. MD software manufacturers started to get in contact and invite tenders for various projects. In fact, to date they have worked on a number of MD software development projects for different types and sizes of manufacturers. Therefore, the overhead required to implement the necessary standards was starting to pay dividends. However, now that the opportunities clearly are out there it is noticeable that BBT now want to move to the next phase of their MD software development journey and not only develop software in line with the MD standards but their ambition is now to increase the efficiency of their MD software development. Therefore, they wish to improve their software development processes even further and implement more regulatory standards in relation to security etc. The key driver to take a step further is that BBT now are undertaking challenging projects and are developing MD software for multinational MD companies they have much more to achieve in their journey. BBT have agreed to work with researchers from the RSRC to introduce MD software development best practices that will increase the efficiency of their MD software development.

Second, BBT realized the increased attention to data security by the regulatory bodies and their USA clients. The increased awareness and value placed on data security by their clients means that implementing strong data protection mechanisms is now a competitive advantage. In addition, if appropriate security controls are not implemented as outlined by HIPAA, it can result in penalties [30, 38]. This can be detrimental to their business and stifle their growth and profits.

A. Challenges for such large projects

However, as with every new project there are associated challenges and this is increased when embarking upon a *fixed price* project, therefore if the project is delayed or runs into some other difficulties, BTT is liable in relation to the budget. Another challenge is the *tight timeframe* where *strict milestones* have to be achieved in addition to the achievement of appropriate documentation to satisfy *regulatory deliverables*. Additionally, BBT would also like to excel in being able to *facilitate change* during the lifecycle of the project as this is something that is challenging in traditional MD software development. A very positive aspect of BBT's current approach is that they engage in regular interaction with their customers. Therefore, receiving feedback and making sure that the right MD software is developed from the very start of the development.

B. What is the current status of BBT development process lifecycle?

Currently BBT is developing software in a plan driven way through using the V-model [19]. When following a V-model the testing is planned in parallel with the corresponding development phase and the planning for verification and validation of the product is emphasized from the very beginning. Even though V-model has been used by BBT successfully and it has been proven to be the best fit when developing MD software in compliance with the regulations [20]. However, in order to improve the efficiency of their software development new software practices should be explored that have proven successful in the development of safety-critical software in association with researchers from the RSRC.

Before introducing a new lifecycle it is crucial to perform an assessment in order to establish how the current software development process should be improved/changed.

VI. ASSESSMENT PROCESS AND RESULTS

The following subsections will describe the high-level assessment process completed in BBT in 2016 and those in progress in 2017.

A) Software Development Process Assessment

The assessment carried out in 2016 was focused on the software development processes.

The Software development process assessment was performed at BBT before deciding what new practices would be most suitable for BBT. We met up with the CEO of the company, project manager/developer (who had has experience of agile software development), and a developer who specialized in Android software development. The meeting was also attended by the R&D manager/Systems Risk engineer and the QMS manager. The assessment was based on previously scripted open-ended questions that related to many different areas of the company as well as the software development process.

Results for the Software Development Process Assessment:

a) Currently BBT have several standards in place, such as IEC 62304, ISO 13485, ISO 9001 and ISO 14971. In their software development process they make use of various tools in areas such as project management, testing and integration. One of their main drivers for adopting new best practice software development methods is to streamline even further their already succcessful practices for interacting with customers. BBT view this as being key to delivering safe regulatory compliant software that fully meets the customer requirements and works within the intended environment, thereby decreasing the chances of expensive rework, particularly on fixed price projects.

b) Additionally, they wish to develop metrics such as problem tracking, code coverage, defects found, defects closed etc.

c) In the past BBT was open to changes and customers able to introduce them whenever they wanted without consequences to the overall budget, time. However, today the process has become more structured. BBT now ensures that a formal change document is in place specifying what happens if a change occurs within a previously signed project.

d) BBT at the moment is not making use of any principle software design techniques however, they plan to introduce architecture diagrams and design patterns.

e) BBT previously have developed software in a plan driven manner and lately they have decided to integrate some agile practices into their development process..

f) At the moment almost 80% of a testing is automated and 20% is done manually. If the percentage of manual testing could be decreased further – the overall development process could be faster. Automation of tests can prove challenging when components such as Bluetooth or Wifi are involved.

g) One of the team members mentioned that due to the new lifecycle approach where agile practices are introduced, there could be a challenges regarding integrating the QMS with the development process and achieving the necessary regulatory documentations.

h) At present their current process incorporates only two agile practices, they are: short iterations (every 2 weeks) and continuous integration.

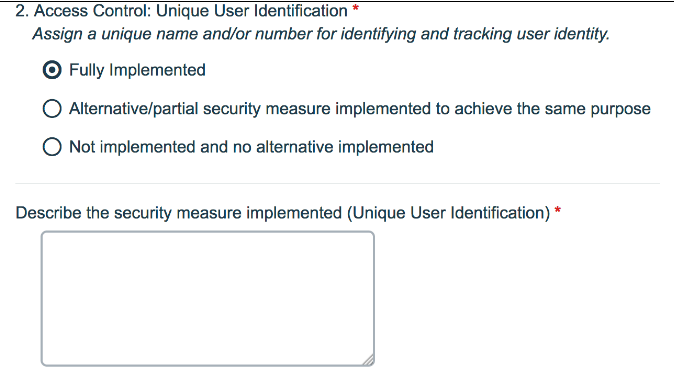
i) BBT is also planning to provide their team with the training needed in order to work in an environment where MD software is developed in an agile way. The team will be provided with training in regards to MD software, agile practices and mobile app development.

j) Some team members will be provided with support to change towards adopting a more agile software development process.

B) Data Protection and Regulation Assessment

This section describes the high-level assessment process currently in progress at BBT in 2017.

BBT currently implements security controls to ensure data security. However, they need to ensure that their controls are inline with the safeguards outlined by HIPAA in order to continue working with their clients in the US. Strengthening data security will have the added advantage of enhancing their competitive advantage, avoid any regulatory risks in the future, and improve longevity within the MD software market. We are first assessing how well BBT's security controls for their software align with HIPAA safeguards. The focus is on the HIPAA safeguards outlined in the Security Rule. We are using a web-based tool to capture whether a particular HIPAA safeguard is either “fully implemented”, or “alternative/partial security measure implemented to achieve the same purpose” or “not implemented and no alternative implemented”. For each response further explanation will be captured to get details of what security control is implemented and how it isimplemented, or alternatively provide an explanation as to why no security control is implemented for a particular safeguard. An example is shown in Figure 2. The HIPAA safeguard shown in the example in Figure 2, “Access Control” is from the HIPAA Security Rule, under the Technical Safeguards.



2. Access Control: Unique User Identification *

Assign a unique name and/or number for identifying and tracking user identity.

● Fully Implemented

○ Alternative/partial security measure implemented to achieve the same purpose

○ Not implemented and no alternative implemented

Describe the security measure implemented (Unique User Identification) *

Figure 2. Assessment against HIPAA Safeguards

The next step will be data analysis and workshop with the developers at BBT to discuss gaps between the HIPAA safeguards and the security controls currently implemented. We will then use IEC/TR 80001-2-8 as a guide for selecting appropriate security controls for BBT to implement in order to address any HIPAA safeguards that are not well addressed. Relevant security risks will be taken into consideration during the process.

VII. RECOMMENDATIONS

A) Agility of Software Development Processes

Our advice to BBT is to integrate more agile practices into their current MD software development so that the software is developed efficiently in regular iterations and can be presented to the customer on a regular basis and facilitate change. Based upon a mini-literature review performed, the following agile practices have been cited as being used to develop software successfully for safety critical/medical domains:

a) Acceptance test-driven development (ATDD) [21].

b) Automated Tests/Automated unit testing [22].

c) Code Reviews / Peer Reviews [23].

d) Coding Standards [21], [24].

e) Continuous integration (CI) [21], [24], [25].

f) Open Workspace [21], [26].

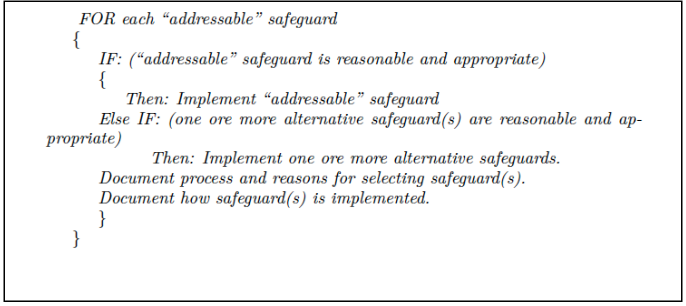
g) Scrum [27].

h) Test-driven development (TDD) [21], [28]

B) Data Security: Adhering to HIPAA During Software Development

The safeguards for EPHI/PHI that can be traced to development work are outlined within the Security Rule [39]. They are outlined under the Technical and Physical Safeguards parts of the Security Rule [39].

The Security Rule has one other part, Administrative Safeguards, but this contains management processes, policies and planning, e.g., risk management and analysis procedures. The Safeguards in the Technical and Physical parts of the Security Rule are either labeled as ``required" or ``addressable" [29, 39]. Those labeled as ``required" must be implemented. They must be included within the requirement specification document just to make sure that they are considered during design, implementation and the verification and validation phases of the software. The safeguards labeled as ``addressable" can be implemented depending on how reasonable and appropriate they are given a particular context, e.g., the software and how it can be used. Alternatively, a different safeguard can be implemented if there are one or more safeguards that would achieve the same or better level of security, and are reasonable and appropriate. Figure 3 and Figure 4 show the steps that we propose for addressing the safeguards in the Technical and Physical Safeguards part of the Security Rule.



```
FOR each "addressable" safeguard
{
    IF: ("addressable" safeguard is reasonable and appropriate)
    {
        Then: Implement "addressable" safeguard
    Else IF: (one ore more alternative safeguard(s) are reasonable and appropriate)
            Then: Implement one ore more alternative safeguards.
    Document process and reasons for selecting safeguard(s).
    Document how safeguard(s) is implemented.
    }
}
```

Figure 4. Implementing Addressable Safeguards

It is important to note that each of the security capabilities in the international standard IEC/TR 80001-2-8 comes with many security controls. But it is not practical or feasible to implement all of the security controls in a software product. This is because some of the security controls many not be relevant given the context or type of software security concerns for the software system. This is why, as suggested by the standard IEC/TR 80001-2-8, the selection of the controls should be based on risk or threat identification and assessment, and most importantly, both patient safety and protection of health information. It is also

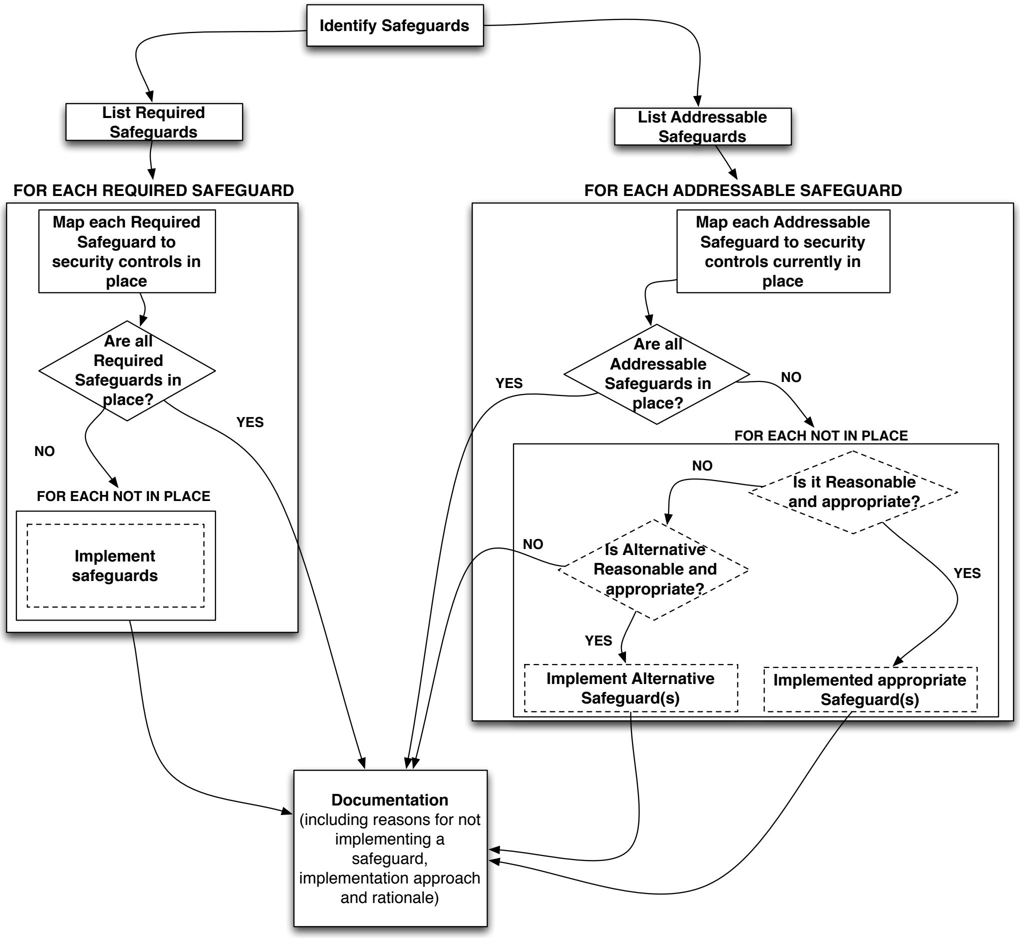

Identify Safeguards
List Required Safeguards
List Addressable Safeguards
FOR EACH REQUIRED SAFEGUARD
Map each Required Safeguard to security controls in place
Are all Required Safeguards in place?
YES
NO
FOR EACH NOT IN PLACE
Implement safeguards
FOR EACH ADDRESSABLE SAFEGUARD
Map each Addressable Safeguard to security controls currently in place
Are all Addressable Safeguards in place?
YES
NO
FOR EACH NOT IN PLACE
Is it Reasonable and appropriate?
NO
YES
Is Alternative Reasonable and appropriate?
NO
YES
Implement Alternative Safeguard(s)
Implemented appropriate Safeguard(s)
Documentation (including reasons for not implementing a safeguard, implementation approach and rationale)

Figure 3. Proposed Approach for Addressing Security Controls for Technical and Physical Safeguards

worth noting that a similar consideration when implementing security controls is also advocated in the HIPAA Security Rule.

Understanding security threats and security weaknesses can help make an informed judgement in relation to the appropriate security controls to implement. Hence, input from a well detailed threat modeling approach will be very useful during the selection process. An overview of threat modeling is provided by The OWASP Foundation [40].

After implementation, maintenance of the safeguards, which should include improvements, should be performed as necessary in order to ensure continued protection of EPHI/PHI. This is particularly important for evolving software. The addition of new features or implementation of defect-fixes, which is part and parcel of software evolution, may affect the efficacy of the implemented safeguards. Therefore, continuous maintenance is necessary to ensure the implemented safeguards keep securing EPHI/PHI.

Our advice to BBT is to assign employees that continuously check compliance with HIPAA regulatory requirements, as well as on identifying and assessing relevant security threats and vulnerabilities. The employees responsibility will be to ensure that appropriate security controls are implemented, not only to comply with data security regulations, but also that relevant security concerns are addressed. The employees should be involved early within the development lifecycle, ideally from requirements elicitation, and continue throughout the evolution of the product. The identification and assessment of threats and vulnerabilities, which is advocated in the HIPAA Security Rule, can be done by following a threat modeling approach. As an example of a threat modeling approach we show in Figure 5 the one proposed by Oladimeji et al. [41]. More details of their well detailed approach can be found in their paper.

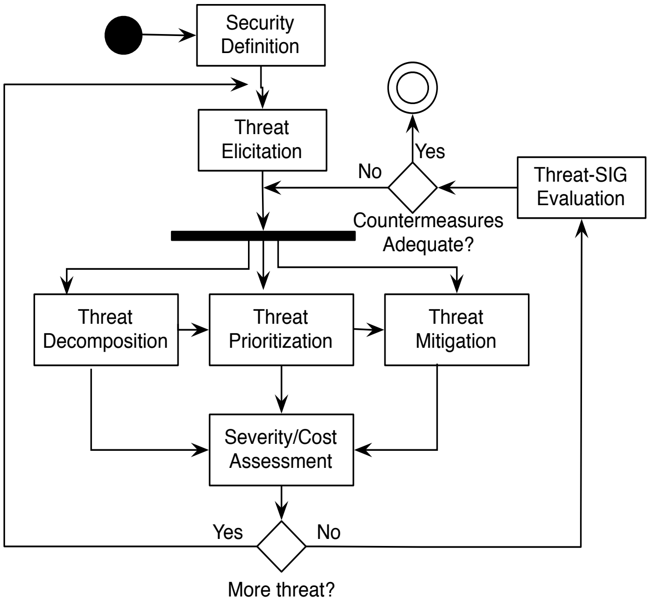


Figure 5. Threat modeling approach proposed by Oladimeji et al. [41]

The advantage for BBT, or any other company, of having dedicated employees that continuously assess compliance with data security regulations and assess threats and vulnerabilities is that it ensures that there is a proactive rather than a reactive process to addressing security concerns. This significantly reduces the likelihood of costly rework and implementing security patches late within the development lifecycle.

VIII. Conclusion and Future Work

This paper describes a case study of a journey taken by an Irish software development company, moving from developing automotive software to developing MD software. We described how through adopting and implementing MD standards they now have become a MD software supplier. Since becoming a MD software supplier many new opportunities have become available. However, BBT now wish to further improve their software development processes in order to become more efficient and to be able to satisfy new challenges that could rise from undertaking new multinational MD manufacturer's projects. They also need to take steps to ensure that their approach to ensuring data security is in line with regulatory requirements. Taking a software engineering approach, the authors of this paper provide a list of agile practices that have been cited to be well suitable for the safety critical/medical domain. The authors have also outlined an engineering approach to help with identifying and implementing appropriate security controls when developing software. The approach will help the company to develop software that is compliant with data security regulations.

In the future, we plan to investigate agile practices that are applicable for the MD software industry in greater detail by performing an extensive literature review and industry survey. Further, we will work with BBT to integrate the most applicable agile practices into their current software development lifecycle. We also plan to assist BBT with addressing data security concerns for the software that they develop. In addition, we will guide them through the process of ensuring that their software complies with HIPAA data regulations, and appropriate security controls are put in place. This is the first time that we are using a web-based tool for the assessment of how well the case company addresses HIPAA safeguards. We will use lessons learned from the process to refine and improve the tool.

Acknowledgment

This research is supported by the Science Foundation Ireland Research Centres Programme, through Lero - the Irish Software Research Centre (http://www.lero.ie) grant 10/CE/I1855 & 13/RC/2094.

References

[1] K. Trektere, F. McCaffery, G. Coady, and M. Gubellini, "Case Study: Becoming a Medical Device Software Supplier," *The Second International Conference on Fundamentals and Advances in Software Systems Integration*, (FASSI), 2016, pp. 24-29.

[2] J. Cunningham, B. Dolan, D. Kelly, and C. Young, "Medical Device Sectoral Overview," *Galw. City Cty. Econ. Ind. Baseline Study*, 2015.

[3] C. Abraham, E. Nishihara, and M. Akiyama, "Transforming healthcare with information technology in Japan: A review of policy, people, and progress," *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 157–170, 2011.

[4] S. Hanna, R. Rolf, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song, "Take two software updates and see me in the morning: The Case for Software Security Evaluations of Medical Devices," in *The 2nd USENIX conference on Health security and privacy*, 2011.

[5] S. R. Rakitin, "Coping with Defective Software in Medical Devices," pp. 40–45, 2006.

[6] EC, "Directive 2007/47/EC of the European Parliament and of the Council concerning medical devices," *Official Journal of the European Union*. Official Journal of the European Union, Brussels, Belgium, p. 35, 2007.

[7] F. McCaffery, J. Burton, A. Dorling, and V. Casey, "Software Process Improvement in the Medical Device Industry," in *Software Engineering Encyclopaedia*, P. Laplante, Ed. New York: Francis Taylor Group, 2010, pp. 528 – 540.

[8] C.-J. Hsiao, E. Hing, T. C. Socey, and B. Cai, "NCHS Health E-Stat Electronic Medical Record/Electronic Health Record Systems of Office-based Physicians: United States, 2009 and Preliminary 2010 State Estimates," *Natl. Cent. Heal. Stat.*, vol. 2009, no. December, pp. 6, 2010.

[9] G. Hillestad, R., Bigelow, J., Bower, A. and F. Girosi, "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs," *Health Aff.*, vol. 24, no. January, pp. 1103–17, 2016.

[10] "Mobile to Play a Significant Role in Healthcare as GSMA Research Predicts mHealth Market to be Worth US$23 billion by 2017," 2012. [Online]. Available: http://www.gsma.com/newsroom/press-release/mobile-to-play-a-significant-role-in-healthcare-as-gsma-research-predicts-mhealth-market-to-be-worth-us23-billion-by-2017/. [Accessed: 26-Mar-2016].

[11] BSI, "Medical device software- Software life-cycle processes, 62304:2006," *Bs En 62304:2006*, vol. 3, 2006.

[12] ISO, "ISO 13485: Medical Devices - Quality Management Systems - Requirements for Regulatory Purposes." Geneva, Switzerland, p. 57, 2003.

[13] ISO, "ISO 14971 - Medical Devices - Application of Risk Management to Medical Devices." Geneva, Switzerland, p. 82, 2009.

[14] F. McCaffery, M. Lepmets, and P. Clarke, "Medical Device Software as a Subsystem of an Overall Medical Device," in *Proceedings of The First International Conference on Fundamentals and Advances in Software Systems Integration Medical*, 2015, pp. 17–22.

[15] IEC, "IEC TR 80002-1 - Medical Device Software - Part 1: Guidance on the Application of ISO 14971 to Medical Device Software." Geneva, Switzerland, p. 58, 2009.

[16] FDA, "Guidance for Industry - FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices." USA, p. 26, 1999.

[17] FDA, "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices." USA, p. 23, 2005.

[18] FDA, "General Principles of Software Validation ; Final Guidance for Industry and FDA Staff." USA, p. 47, 2002.

[19] K. Forsberg and H. Mooz, "The Relationship of System Engineering to the Project Cycle," *12th INTERNET World Congr. Proj. Manag.*, no. June 1994, p. 12, 1994.

[20] F. McCaffery, D. McFall, P. Donnelly, F. G. Wilkie, and R. Sterritt, "A Software Process Improvement Lifecycle Framework for the Medical Device Industry," in *IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'05) Proceedings*, 2005, p. 8.

[21] S. Datta, P. Sarkar, S. Das, S. Sreshtha, P. Lade, and S. Majumder, "How many eyeballs does a bug need? An empirical validation of linus' law," in *Lecture Notes in Business Information Processing*, 2014, vol. 179 LNBIP, pp. 242–250.

[22] J. Grenning, "Launching extreme programming at a process-intensive company," *IEEE Softw.*, vol. 18, no. 6, pp. 27–33, 2001.

[23] M. Bernhart, A. Mauczka, and T. Grechenig, "Adopting code reviews for agile software development," in *Proceedings - 2010 Agile Conference, AGILE 2010*, 2010, pp. 44–47.

[24] K. Beck, *Extreme Programming Explained*. 1999.

[25] P. Dahlem, Marc and Diebold, "Agile Practices in Practice - A Mapping Study Agile Practices in Practice - A Mapping Study -," in *18th International Conference on Evaluation and Assessment in Software Engineering*, 2015, no. MAY 2014.

[26] K. Beck, "Embracing change with extreme programming," *Computer (Long. Beach. Calif).*, vol. 32, no. 10, pp. 70–77, 1999.

[27] P. Abrahamsson, O. Salo, J. Ronkainen, and J. Warsta, *Agile software development methods Review and analysis*. ESPOO: VTT Publications 478, 2002.

[28] J. Rasmusson, *The Agile Samurai, How Agile Masers Deliver Great Software*. Texas, 2010.

[29] The Health Insurance Portability and Accountability Act

(HIPAA) of 1996. Pub. L. 104-191. Stat. 1936.

[30] Brief OCR Privacy. "Summary of the HIPAA Privacy Rule." Washington, DC, United States Department of Health and Human Services, 2005.

[31] IEC 80001-2-8 - Application of risk management for it networks incorporating medical devices – part 2-8: Application guidance – guidance on standards for establishing the security capabilities identified in IEC 80001-2-2. International Electrotechnical Committee, pages 43.

[32] IEC 80001-2-2 - Application of risk management for it-networks incorporating medical devices-guidance for the disclosure and communication of medical device security needs, risks and control. International Electrotechnical Committee, pages 48.

[33] NIST, SP. "800-53." Recommended Security Controls for Federal Information Systems: 800-53, 2013.

[34] ISO/IEC 15408-2:2008 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components. *International Organization for Standardization / International Electrotechnical Committee*, pages 218.

[35] ISO/IEC 15408-3:2008 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components. *International Organization for Standardization / International Electrotechnical Committee*, pages 174.

[36] IEC 62443-3-3:2013 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. International Electrotechnical Committee, pages 80.

[37] ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls. International Organization for Standardization / International Electrotechnical Committee, pages 80.

[38] S. Hoffman and A. Podgurski, "Securing the HIPAA Security Rule. Journal of Internet Law", Spring 2007; Case Legal Studies Research Paper No. 06-26.

[39] TrueVault, HIPAA compliance developer guide. TrueVault, 2014. Retrieved from https://github.com/truevault/hipaa-compliance-developers-guide. Accessed on 27th Februrary 2017.

[40] OWASP Foundation "Threat Risk Modeling", Retrieved from https://www.owasp.org/index.php/Threat_Risk_Modeling. Accessed on 27th Februrary 2017.

[41] E. A. Oladimeji, S. Supakkul, and L. Chung. "Security threat modeling and analysis: A goal-oriented approach." Proc. of the 10th IASTED International Conference on Software Engineering and Applications (SEA 2006). 2006.