The Need for Trustworthiness Models in Healthcare Software Solutions

Raja Manzar Abbas[1], Noel Carroll[1,2], Ita Richardson[1,2] and Sarah Beecham[1]

[1]*Lero- The Irish Software Research Centre, University of Limerick, Limerick, Ireland*

[2]*ARCH- Applied Research for Connected Health Technology Centre, University of Limerick, Limerick, Ireland*

Keywords: Trustworthiness, Healthcare Software, Trustworthiness Attributes.

Abstract: Trustworthiness in software is of vital importance to technology users, especially in health, where lives may depend on the correct application of software that is fit for purpose. Despite the risk posed by improper use of technology in the health domain, there is evidence to suggest that stakeholders often trust the software without fully appreciating the possible consequences. In this paper, we explore what determines trustworthiness in healthcare software solutions. While there are often claims of improved quality of care, increased safety and improved patient outcomes using healthcare technology – the scientific basis for such claims appear to be uncritically accepted. Ultimately, this can lead to a surge in healthcare software solutions, some of which may be misaligned with healthcare needs and potentially lead to fatal outcomes. To support health technology stakeholders, we propose a 'trustworthiness healthcare software model' that can be employed to assess the level of trustworthiness associated with healthcare software solutions.

1 INTRODUCTION

The United Nation's International Standard Industrial Classification, (2016) categorizes healthcare as generally consisting of hospital activities, medical and dental practice activities. Implementations of potentially transformative healthcare technologies are currently underway internationally, often with significant impact on national expenditure. For example, Ireland has invested approximately €900 million in its e-health while the UK has invested at least £12.8 billion in a National Programme for Information Technology (NPfIT) for the National Health Service. Similarly, the Obama administration in the United States has committed to a US$38 billion Healthcare investment (Catwel et al., 2009).

Such large-scale expenditure has been justified on the grounds that electronic health records (EHRs), picture archiving and communication systems (PACS), electronic prescribing (ePrescribing) and associated computerised provider (or physician) order entry systems (CPOE), and computerised decision support systems (CDSSs) will help address the problems of variable quality, safety and trust in the modern health care. However, the scientific basis of achieved quality and trust – which are repeatedly made and are seemingly uncritically accepted – remains to be established (Huckvale et al., 2012; Institute of Medicine, 2007).

1.1 Problem Statement

The ultimate goal of software is to help end-users to accomplish their tasks in a convenient and efficient manner. However, the literature suggests that software technology advancements in healthcare often failed to ease the lives of the healthcare professionals. Instead, healthcare professionals often report a loss of productivity while using healthcare software. This leads to a lack of trust in the healthcare software (Velsen et al., 2016).

1.2 Research Question

In this paper we examine the literature on trustworthiness in healthcare and look particularly at the associated attributes. We also explore the need for a healthcare software model of trustworthiness. Considering the broad and vast nature of software technology use in healthcare, we argue that stakeholders need to have a set of criteria by which they can assess the level of trustworthiness of a given technology.

Abbas R., Carroll N., Richardson I. and Beecham S.
The Need for Trustworthiness Models in Healthcare Software Solutions.
DOI: 10.5220/0006249904510456
In *Proceedings of the 10th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2017)*, pages 451-456
ISBN: 978-989-758-213-4

There is an apparent lack of insight into what a trustworthiness healthcare software model should capture, and how it should be applied. To address these gaps, we formulate the following research questions:

- *RQ1*. What are the key attributes that define trustworthiness of healthcare software?
- *RQ2*. What are the current models or frameworks that capture trustworthiness of healthcare technology?

1.3 Methodology

To explore these questions, we undertook a structured literature review. A structured literature review may be described as appraisals of past studies conducted systematically, purposefully and methodologically (Armitage and Keeble-Allen, 2008; Petticrew, 2001).

In the research discussed in this article, a literature search was completed in the bibliographic databases ACM Digital Library, IEEE, Springer LINK and Google Scholar, using the keyword search phrases '*trustworthiness*', '*healthcare software*', '*healthcare trust*', '*trustworthiness models', trustworthiness frameworks'*, '*trust attributes'*, '*trustworthy attributes*', '*software trustworthiness*' and '*healthcare software trustworthiness*'. *2894* initial reference sources were found. From these, after screening titles and abstracts , *2224* were deemed not eligible. Out of remaining *670* research articles, *536* articles were screened out after applying the exclusion criteria on the titles and abstracts - *238* were not relevant to software engineering, *107* research articles had no specific intervention about software trustworthiness (trustworthy, trust), *187* articles did not mention software attributes and/or models and *4* research articles were not written in English. After reviewing the full text of the remaining *134* studies, *83* more studies were excluded due to lack of relevance to the topic and *51* studies were selected as primary studies.

2 IMPACT OF HEALTHCARE TECHNOLOGY

Due to the growth in population and shift in demographics, there is a significant pressure on the global healthcare system. Shojania et al. (2016), attribute a toll to medical error of 251,454 deaths in US hospitals per year, making, they say, medical error the third-leading cause of death in the USA. The Institute of Medicine study estimated the cost of nonfatal medical errors is between $17 billion and $19 billion each year, and that between 2.9% and 3.7% of all patients admitted suffer some type of injury because of medical mismanagement. As a result, there is a growing focus on healthcare technology to offer greater service efficiency and it has given rise to a comprehensive sociotechnical model for managing healthcare through software solutions.

Technological advances have encouraged the development of new technologies that drive connectivity across the healthcare sector—apps, gadgets, and systems that personalize, track, and manage care using just-in- time information exchanged through various patient and community connections (Leroy et al., 2014).

This paradigm shift heavily emphasizes the process of software development in healthcare systems. It has also contributed to a shift in healthcare practice, highlighting our growing reliance and trustworthiness of software to support healthcare decisions. However, trusting the healthcare software solution without validating can have serious and potentially fatal consequences (Carroll, 2016).

3 TRUSTWORTHINESS – WHO CARES?

Trustworthiness in healthcare software is the sum of trust in different factors. The composition these factors can differ for different healthcare users. For example, for patients, trustworthiness in software consists of, mostly, a perceived level of control and privacy, while for healthcare professionals, a larger and different set of issues play a role, including reliability and a transparent data storage policy. The set of factors that affect trustworthiness in a healthcare portal are different from the sets that have exist for general software domain. There is a need to study trustworthiness in healthcare software as a separate subject to inform the design of reliable interventions.

3.1 Need for Trustworthiness Healthcare Software Model

With significant growth in healthcare software solutions, software is having an increasing impact on clinical decisions and diagnosis. However, there is little evidence as to the trustworthiness of software. For example, a glitch in St. Mary's Mercy Medical Centre's (Cork, Ireland) patient management system "killed" 8,500 patients on paper (National Computer Security Center, 1985). When St. Mary's upgraded its patient management software, there was a mapping error in the alteration process that triggered the program to notify 8,500 patients of their incorrect death.

While unregulated medical devices rarely find their way to patients, the same cannot be said about the largely unregulated market for health applications and software. As such, in reality, there exists a considerable gap between the potential benefits that software's could provide, and what healthcare professionals are currently likely delivering in practice. Recent reviews in the therapeutic areas of bulimia (Nicholas et al., 2015), asthma (Huckvale et al., 2012), Post-traumatic stress disorder (PTSD) (Olff, 2015), insulin dosing (Huckvale, 2015) and suicide prevention (Larsen et al., 2016) have yielded worrying conclusions regarding the quality, scientific basis and often blatant disregard for safety (The Daily Mail, 2014),

These errors go some way to illustrating the need for trustworthy healthcare software. Although different researchers have tried to address some attributes of trustworthiness not all attributes have been identified. We discuss some of the models and standards and the attributes they cover in an effort to understand what areas they are lacking in.

3.2 Impact of Trustworthiness on Quality

The number of medical errors caused by devices (which have embedded software) and software applications naturally leads to the questions:

- How can healthcare software be made trustworthy?
- What process/mechanism would achieve this?
- How do we inform users and healthcare providers which healthcare software solution can be trusted and why?

We first identified the attributes of trustworthy healthcare software and why there is a need for a trustworthy healthcare software model.

4 DEFINING TRUSTWORTHINESS

According to Merriam–Webster Dictionary (2004), trustworthy means '*worthy of confidence*'. For software products, researchers and practitioners have a slightly different understanding of '*trustworthy software systems*', since we need to view trustworthiness over time.

Trustworthiness is defined by Amoroso et al. (1994) as a "*level of confidence or degree of confidence*" and software trustworthiness is defined as a "*degree of confidence that the software satisfies its requirements*". Since the definition is expressed as a "*degree of confidence*", Amoroso and Taylor illustrates trustworthiness is dependent upon management and technical decisions made by individuals or groups of individuals evaluating the software. Software trustworthiness is expressed in terms of a set of requirements, where the 'set' is variable. For example, trustworthiness may be dependent on the set of functional requirements, or may be a critical subset of functional requirements, or it may be some set of requirements that include non-functional assurance requirements like safety or security (Amoroso et al., 1994).

In his ICSE 2006 Keynote speech, Boehm (2006) pointed out the increasing trend of software criticality and dependability as one of the key software trends. Over the past 50 years, different strategies such as formal methods, security assurance techniques, defect prediction, failure mode and effects analysis, testing methods, and software assurance techniques have been proposed to address different aspects of software trustworthy challenges. Based on these studies, numerous quality categories and attributes have been studied as major factors influencing on software trustworthiness. Among them are included functionality, reliability, safety, usability, security, portability, and maintainability, etc.

In addition, Zhang et al. (2012) reviews the appropriateness of the software attributes summarized by Yang et al. (2009), and suggests that the trustworthiness of software is related to the following set of properties which they redefined to address the trustworthiness context as:

- Safety
- Validity
- Reliability
- Reusability
- Scalability
- Maintainability
- Performance

Carbone et al. (2013) defined trustworthiness from information and communication technology (ICT) systems where security challenges include both confidentiality (or privacy) and in integrity (or trust) of the data. In particular, the notion of trustworthiness seems relevant for tagging databases and electronic patient records with information about the extent to which test results, diagnoses and treatments can be trusted.

Initial findings from literature suggest a lack of understanding of trustworthiness in the healthcare software domain and a need for a trustworthiness process model that define standards or best practices about the trustworthiness of healthcare software.

In this position paper, we propose the key attributes that define trustworthiness of healthcare software and current models that capture trustworthiness of healthcare technology.

5 THEORETICAL FOUNDATIONS

Though there is a growing consensus that trustworthiness is characterized as one that satisfies a collection of critical quality attributes, yet, there is a lack of common understanding of healthcare software trustworthiness – particularly in a healthcare context. Based on the literature and the sample of definitions introduced here, we identify that the key factors of trustworthiness for healthcare software should be regulation, confidence of the users and meet its requirements and objectives in a satisfactorily manner.

5.1 Theoretical Influences on Developing a Trustworthiness Healthcare Software Model

The Capability Maturity Model Integration (CMMI) guides organisations with a view to ensuring that the correct software is being developed throughout each stage in the development cycle and conforms to specification. However, it is important to realise that software process models, such as CMMI, do not cover healthcare regulations, and that they need to be used in conjunction with the regulations (Burton et al., 2006).

There have been some new developments in this area, for example the development of MDevSPICE (formally known as MediSPICE) (Clarke et al., 2014; McCaffery et al., 2010). The MDevSPICE framework is one of the first attempts to address the safety concerns faced by healthcare software producers and presents a software safety assessment process. Verification and validation activities are very important in software development and can consume much of a project's costs and effort. While verification and validation are addressed by process models and standards for both generic and safety critical software development, there are still challenges in undertaking its successful implementation as part of the software development process. The process of verification and validation requires a clear understanding of how each activity is undertaken and related to each other, which is important in a healthcare environment (Carroll and Richardson, 2016).

For example, the development of an international software process improvement (SPI) framework for the medical device industry acts as a key enabler of best practice for the healthcare sector. SPI techniques offer a continuous cycle of performing an assessment and restarting the cycle (McHugh et al., 2012) with the aim of reducing defective software. Software may also be vulnerable to outside attack. Many hospitals and healthcare facilities use various threat management software and firewalls to monitor their mobile device applications to ensure that they are secure and safe. In most cases, within the USA, this is a requirement of Health Insurance Portability and Accountability Act (HIPPA).

HIPAA is a framework which is followed by number of organisations for maintaining the security and privacy of the health information. HIPAA came into force in 1996 to address a number of concerns, most notably the need for increased protection of the medical records of the patients against unauthorised access (Wu et al., 2012). HIPAA provides a national standard for electronic healthcare transactions. It also provides regulations regarding healthcare information security and privacy (Jepsen, T, 2003). HIPAA covers entities such as healthcare providers, insurers and providers of health plan. Healthcare organisations are now required to individually assess their security and privacy requirements using various auditing tools. Healthcare technology systems have access to personal identifiable information.

Our traditional view of privacy protection methods through various anonymization techniques does not provide an efficient way to deal with the privacy of technological healthcare software solutions. For example, in response to growing concerns on privacy and data security, in 2014, the European Commission published a Green Paper on mHealth (European Commission, 2014). Through wide stakeholder consultation, the paper discusses the main barriers and issues related to mHealth deployment. They highlight a number of key topics including data protection, security of health data, informed consent, big data management, patient safety and transparency of information across the EU and, ultimately, on the need to regulate mHealth applications.

One of the main concerns across industry is the lack of a unified model which can incorporate all of the best practices for healthcare software development. There is a need to formulate a healthcare software model that can accurately propagate trustworthiness throughout the process.

5.2 Towards Developing a Trustworthiness Healthcare Software Model

By carefully reviewing the appropriateness of the attributes summarized through a software lens, we suggest that the trustworthiness of healthcare software model is related to the following set of properties:

- **Security:** inclusion of security mechanisms in the model with respect to access control processes.
- **Efficiency:** effectiveness of the model construction that is able to give a quick response or reaction with minimal resources and/or time taken.
- **Safety:** inclusion of semantics that represent process requirements related to safety, and the ability to highlight inconsistencies in the process model with respect to safety-related processes.
- **Functionality:** the functions at the level expressed in functional requirements of the model, emphasizing at the level of final user functionality
- **Reliability:** the probability of the process model delivering results that is consistent with the model assumptions.
- **Regulation:** decision support reference model that will ensure that healthcare software products are safe and effective to protect and promote public health through various standards and regulations.
- **Validity:** the ability of the process model to reflect the assumptions and constraints about the software process specified by process stakeholders.
- **Accuracy:** the measurement tolerance, or transmission of the process model that defines or removes the limits of the errors.

6 FUTURE RESEARCH

Having established a foundation for the Trustworthiness Healthcare Software Model by identifying the key attributes of trustworthiness from a healthcare software perspective, we will continue to build on this to establish key processes and metrics within the model.

As part of our future research, we will examine and modify existing trustworthiness models. The subsequent focus will be on extending and modifying existing techniques based on our identified attributes for the analysis. Then our next step will be to take the trustworthiness model that we develop, to test and refine it on a large scale with healthcare software sector. This way, we will also be able to say which attributes are the most important.

7 CONCLUSIONS

The primary goal for adopting healthcare software is to provide patients the best service possible by gathering and interpreting accurate information. This should help them to take correct and timely decisions which reduces cost, time and effort, thereby resulting in the timely treatment of the patient. But, there are apparent concerns regarding whether we can trust healthcare software solutions.

We have identified that there is a gap, and therefore, a consequent need to introduce a Trustworthiness Healthcare Software Model. In this study, we have focused on an initial definition of trustworthiness attributes from literature. We highlight our next steps towards the development of the Trustworthiness Healthcare Software Model and its validation across the healthcare software sector.

ACKNOWLEDGEMENTS

“This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie)”.

REFERENCES

Amoroso, E., Taylor, C., Watson, J. and Weiss, J., 1994, November. A process-oriented methodology for assessing and improving software trustworthiness. *In Proceedings of the 2nd ACM Conference on Computer and communications security pp. 39-50.*

Armitage, A and Keeble-Allen, D. 2008."Undertaking a structured literature review or structuring a literature review: Tales from the field", Electronic Journal of

Business Research Methods 6 (2), pp. 103-114. Available www.ejbrm.com.

Boehm, B., 2006, May. A view of 20th and 21st century software engineering. *In Proceedings of the 28th international conference on Software engineering pp. 12-29*. ACM.

Burton, J., McCaffery, F. and Richardson, I., 2006, May. A risk management capability model for use in medical device companies. *In Proceedings of the 2006 international workshop on Software quality pp. 3-8.*ACM.

Carbone, M., Christensen, A.S., Nielson, F., Nielson, H.R., Hildebrandt, T. and Sølvkjær, M., 2013, August. ICT-powered Health Care Processes. *In International Symposium on Foundations of Health Informatics Engineering and Systems pp. 59-68*. Springer Berlin Heidelberg.

Carroll, N. 2016. *Key Success Factors for Smart and Connected Health Software Solutions, Computer, Vol. 49, No. 11, pp. 32-38.*

Carroll, N. and Richardson, I., 2016. Software-as-a-Medical Device: Demystifying Connected Health Regulations. *Journal of Systems and Information Technology, 18(2).*

Catwell, L. and Sheikh, A., 2009. Evaluating eHealth interventions: the need for continuous systemic evaluation. *PLoS Med, 6(8),* p.e1000126.

Clarke, P., Lepmets, M., McCaffery, F., Finnegan, A., Dorling, A. and Flood, D., 2014, November. MDevSPICE-a comprehensive solution for manufacturers and assessors of safety-critical medical device software. *In International Conference on Software Process Improvement and Capability Determination pp. 274-278*. Springer International Publishing.

European Commission (2014), "Green paper on mobile health ('mHealth')", COM 219 final, SWD 135 Final, available at: http://ec.europa.eu/digital-agenda/en/ news/green-paper-mobilehealth- *mhealth (accessed November, 2016).*

Huckvale, K., Adomaviciute, S., Prieto, J.T., Leow, M.K.S. and Car, J., 2015. Smartphone apps for calculating insulin dose: a systematic assessment. *BMC medicine, 13(1*), p.1.

Huckvale, K., Car, M., Morrison, C. and Car, J., 2012. Apps for asthma self-management: a systematic assessment of content and tools. *BMC medicine, 10(1), p.1.*

Huckvale, K., Car, M., Morrison, C. and Car, J., 2012. Apps for asthma self-management: a systematic assessment of content and tools. *BMC medicine, 10(1), p.1.*

Institute of Medicine (2007) *Preventing medication errors*. Washington (D.C.): National Academy Press.

Jepsen, T., 2003. IT in healthcare: progress report. IT professional, 5(1), pp.8-14.

Larsen, M.E., Nicholas, J. and Christensen, H., 2016. A systematic assessment of smartphone tools for suicide prevention. *PloS one, 11(4)*, p.e0152285.

Leroy, G., Chen, H. and Rindflesch, T.C., 2014. Smart and connected health. *IEEE Intelligent Systems, 29(3), pp.2-5.*

McCaffery, F., Dorling, A. and Casey, V. (2010), *"Medi SPICE: an update"*, available at: http:// eprints.dkit.ie/48/ (accessed 14 November 2016).

McHugh, M., McCaffery, F. and Casey, V., 2012. Software process improvement to assist medical device software development organisations to comply with the amendments to the medical device directive. *IET software, 6(5), pp.431-437.*

Merriam-Webster, 2004. *Merriam-Webster's Collegiate Dictionary*. Merriam-Webster.

Nicholas, J., Larsen, M.E., Proudfoot, J. and Christensen, H., 2015. Mobile apps for bipolar disorder: a systematic review of features and content quality. *Journal of medical Internet research, 17(8).*

Olff, M., 2015. Mobile mental health: A challenging research agenda. *European journal of psychotraumatology, 6.*

Petticrew, M.A. (2001)."Systematic literature reviews from astronomy to zoology: Myths and misconceptions", *British Medical Journal 322 (7278), pp. 98-101*. Available www.bmj.com/cgi/contact/full/322/7278/98.

Shojania, K.G. and Dixon-Woods, M., 2016. Estimating deaths due to medical error: the ongoing controversy and why it matters. *BMJ Quality & Safety, pp.bmjqs-2016.*

The Daily Mail: *Health warning over blood pressure monitoring apps as doctors warn they are 'untested, inaccurate and potentially dangerous'*. Available at: http://www.dailymail.co.uk/sciencetech/article-2887791/Health-warning-blood-pressure-apps-doctors-warn-untested-inaccurate-potentially-dangerous.html.

United Nations. *International Standard Industrial Classification of All Economic Activities, Rev.3.* New York.

Van Velsen, L., Wildevuur, S., Flierman, I., Van Schooten, B., Tabak, M. and Hermens, H., 2016. Trust in telemedicine portals for rehabilitation care: an exploratory focus group study with patients and healthcare professionals. *BMC medical informatics and decision making, 16(1), p.1.*

Wu, R., Ahn, G.J. and Hu, H., 2012, January. Towards HIPAA-compliant healthcare systems. *In Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium pp. 593-602.* ACM.

Yang, Y., Wang, Q. and Li, M., 2009, May. Process trustworthiness as a capability indicator for measuring and improving software trustworthiness. In *International Conference on Software Process pp. 389-401*. Springer Berlin Heidelberg.

Zhang, H., Kitchenham, B. and Jeffery, R., 2012. Toward trustworthy software process models: an exploratory study on transformable process modeling. *Journal of Software: Evolution and Process, 24(7), pp.741-763*.