The Importance of Health Informatics in Public Health during a Pandemic
J. Mantas et al. (Eds.)

Safety Justification of Healthcare Applications Using Synthetic Datasets

George DESPOTOU [a,1], Stuart HARRISON [a],
Sean WHITE [b] and Theodoros N ARVANITIS [a]
[a] *Institute of Digital Healthcare, WMG, University of Warwick, UK*
[b] *Clinical Safety Team, NHS Digital, UK*

Abstract. *Background:* Increasing numbers of intelligent healthcare applications are developed by analysing big data, on which they are trained. It is necessary to assure that such applications will be safe for patients; this entails validation against datasets. But datasets cannot be shared easily, due to privacy, and consent issues, resulting in delaying innovation. Realistic Synthetic Datasets (RSDs), equivalent to the real datasets, are seen as a solution to this. *Objective:* To develop the outline for safety justification of an application, validated with an RSD, and identify the safety evidence the RSD developers will need to generate. *Method:* Assurance case argument development approaches were used, including high level data related risk identification. *Result:* An outline of the justification of such applications, focusing on the contribution of the RSD. *Conclusions:* Use of RSD will require specific arguments and evidence, which will affect the adopted methods. Mutually supporting arguments can result in a compelling justification.

Keywords. Safety, assurance, realistic synthetic dataset, clinical decision support

1. Introduction

Advances in technologies have resulted in numerous intelligent healthcare applications, providing advice, support as well as diagnosis. Failures in their operation may cause harm to patients, by offering incorrect advice, or by making the wrong diagnosis. This is increasingly recognised in regulation and standards, where they are seen as medical devices [1], [2], in need of safety assurance [3]. Developers are often asked to articulate the justification of their application's safety, known as an assurance case (e.g., UK NHS DCB0160 and DCB0129). Assurance cases provide a means of explaining how evidence created during development and validation, can allow to claim that an application is acceptably safe. Effective assurance of intelligent applications will require validation, by testing the application using datasets, representative of the clinical scenarios in which they are used. However, datasets cannot be freely used for validation, as they may result in compromising the privacy of patients. The use of Realistic Synthetic Datasets (RSDs) is seen as a way to overcome this and encourage innovation [4], [5]. The paper presents the outline of an assurance justification of an intelligent application, using the RSD based approach. The assurance framework provides the aspects that need to be justified, and expected types of evidence, in order for an RSD based approach to be used confidently

[1] Corresponding Author, George Despotou, Institute of Digital Healthcare, WMG, University of Warwick, CV4 7AL, UK; E-mail: g.despotou@warwick.ac.uk.

for the validation of intelligent applications. The framework was used to elicit requirements for appropriate statistical evidence for the use of RSD, in a proof of concept project on generating realistic synthetic datasets for application validation.

2. Safety Justification of the of the Synthetic Dataset

Figure 1 shows the identified assurance justification outline, for of an intelligent healthcare application following the process in [6]. Claims are expressed as post conditions [7], supported by a series of further claims, until they can be supported by evidence.

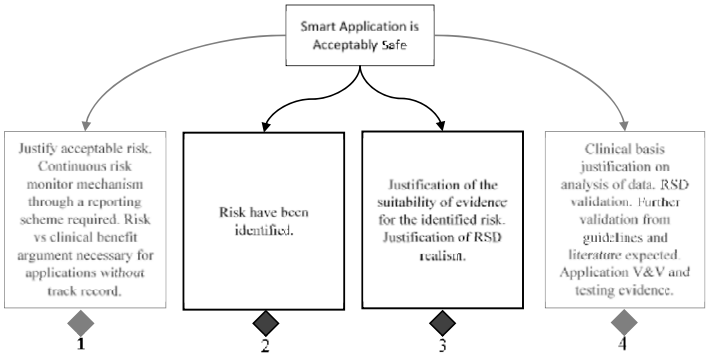

Figure 1. Justification outline (claim and supporting arguments) for an intelligent healthcare application (arguments #2 and #3 are relevant to RSD), loosely using the Goal Structuring Notation that is common in safety cases. Diamonds denote that the argument need to be further developed.

A high level claim about assurance is supported by four arguments : a) description of the acceptable residual risk, which will eventually need to be balanced against expected clinical benefit (arg. #1); b) justification of correctness of the application, including testing results, and validation against the RSD (arg. #4); c) justification placing our confidence in the claim made by argument #4 (arg. #3); and d) justification that the application risks have been identified, including the risks of using an RSD (arg. #2).

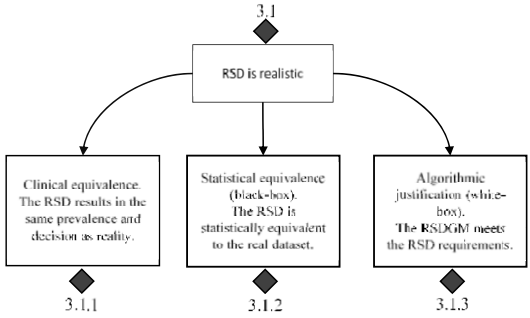

Figure 2. Justification for the realism of the Realistic Synthetic Dataset (RSD).

Figure 2 illustrates the expected arguments of the justification for claiming that the RSD is realistic. There are three arguments identified: a) the RSD results in a dataset that represents realistically clinical knowledge (e.g., prevalence of a disease), as well as outliers; b) statistical equivalence of the real and the synthetic datasets; and c) the employed generation methods are fit to satisfy the RSD usage requirements. The

statistical equivalence looks at the approach as being a black box, only comparing the resultant RSD with the real dataset. However, applications that may be highly critical (e.g., secondary care CDS, or large numbers of patients exposed to the risk), a justification of the RSDGM itself may be necessary to provide sufficient assurance. Tolerance of difference between the two datasets will need justification in the context of specific applications.

3. Establishing the Risk of using the Synthetic Dataset

Risk identifies the safety significance of failures that may affect the users of a service. A safety analysis process will aim to eliminate, or reduce their risk to acceptable levels. Achieving this requires identification of the failures, and their likelihood and severity. Table 1 summarizes a top-down identification of failures that may be caused due to the RSD [8], which are expected to be found in argument #2.

Table 1. Failure modes applying the RSD, to be considered when using the RSD for application validation.

RSD Failure Modes	Description
Unrealistic	The resultant dataset contains data, based on which, any inferences would be wrong or beyond a certain tolerance when compared to reality.
Coverage	RSD does not detect inferences for border cases and outliers.
Underrepresent	Minority populations not sufficiently represented in the synthetic dataset.
Unwarranted	The resultant dataset creates inferences unwarranted in the real data.

In the context of validating a healthcare application (figure 1), failure modes may: a) detect a wrong recommendation (undetected error); b) suggest a false negative on a recommendation by the application (undetected inference); c) provide false assurance that a minority population is covered; and d) falsely suggest that the application should have provided a recommendation (unwarranted inference).

4. Evidence Supporting Assurance of the Synthetic Dataset

The arguments supporting the claim about the realism of the RSD, will require different types of evidence (Table 2).

Table 2. Potential evidence suitable to support the arguments for the realism of the RSD (Figure 2)

Argument	Evidence
3.1.1 – Clinical equivalence	Expert clinical review, comparison with literature, coverage and quality of the real data, persona-based testing, outlier testing.
3.1.2 – Statistical equivalence	Divergence metrics for probability distributions, cross-correlation matrix between the two datasets, non-parametric statistical significance,
3.1.3 – Algorithmic justification	Hyperparameter configuration, probability graphs, divergence metrics minmax proof.

The clinical equivalence argument (3.1.1) is expected to provide independent support to the other branches, by not only focusing on comparison of the two datasets, but comparing the RSD with reality. This way we can identify problems that the two other arguments may not reveal. It will also encourage identification of counter evidence, overcoming potential confirmation bias. Persona-based scenarios allow testing for outliers and minority representation, based on experts' knowledge and literature. The statistical equivalence argument (3.1.2) focuses on evidence of suitability of the RSD to be used in lieu of the real dataset. This can be challenging, as the purpose of the RSD is to diverge from the real dataset, in order to preserve privacy. Finally, the algorithmic

argument (3.1.3) offers evidence about the RSDGM. This is the branch that is most dependent on the adopted method. Methods, such as probabilistic graphs, offer more visibility than neural network approaches (e.g., Generative Adversarial Networks).

5. Conclusions

Realistic synthetic datasets are a promising approach, for validation and safety assurance of intelligent healthcare applications. This will overcome barriers of using real datasets due to privacy concerns, enabling development of applications that may increase patient benefit. The paper presented an outline for the justification of such an application, validated specifically with an RSD. This allows the RSD developers to understand the implications of assurance on the generation process. The framework allowed to identify design and validation requirements, for an RSD generation method, in a proof of concept project.

Acknowledgements & Notes

This work was performed in collaboration with the NHS Digital, under the £10m Regulators' Pioneer Fund, that the MHRA has been awarded. The fund was launched by The Department for Business, Energy and Industrial Strategy (BEIS) and administered by Innovate UK. The fund enables UK regulators to develop innovation-enabling approaches to emerging technologies and unlock the long-term economic opportunities identified in the government's modern Industrial Strategy. This is work is research and does not reflect future policies nor recommendations of the involved organisations.

References

[1] MHRA, Guidance: Medical device stand-alone software including apps (including IVDMDs). Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/718765/Software_flow_chart_Ed_1-05.pdf (10/10/2019)

[2] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[3] FDA, Clinical Decision Support Software Draft Guidance for Industry and Food and Drug Administration Staff. Available: https://www.fda.gov/media/109618/download (10/10/2019).

[4] Walonoski J, Kramer M, Nichols J, Quina A, Moesel C, Hall D, Duffett C, Dube K, Gallagher T, McLachlan S, Synthea: An approach, method, and software mechanism for generating synthetic patients and the synthetic electronic health care record, JAMIA 25(3) (2018), 230-238, doi: 10.1093/jamia/ocx079.

[5] Pollack AH, Simon TD, Snyder J, Pratt W, Creating synthetic patient data to support the design and evaluation of novel health information technology, doi: 10.1016/j.jbi.2019.103201.

[6] Despotou G, Ryan M, Arvanitis TN, Rae AJ, White S, Kelly T, Jones RW, A framework for synthesis of safety justification for digitally enabled healthcare service, Digital Health 3 (2017), doi: 10.1177/2055207617704271.

[7] Despotou G, White S, Kelly T, Ryan M, Introducing safety cases for health IT, 2012 4th International Workshop on Software Engineering in Health Care (SEHC) (2012), 44-50. doi: 10.1109/SEHC.2012.6227010.

[8] SCSC, Data Safety Guidance, The Data Safety Initiative Working Group [DSIWG], ISBN-13:978-1981662463, Available: https://scsc.uk/r127C:2?t=1 (10/10/2019).