Understanding and de-risking the dependencies between operator and manufacturer of clinical IT

George DESPOTOU[a,1], Theodoros N. ARVANITIS[a], Sean WHITE[b]
[a]*Institute of Digital Healthcare, WMG, University of Warwick. UK*
[b]*Health and Social Care Information Centre (HSCIC), UK*

Abstract. Health IT, in addition to benefits can also have unintended consequences both in terms of operational and business risks. Understanding the dependencies between operator and manufacturer as well as issues that need to be addressed during procurement is essential to increase confidence in the operation of health IT. The paper provides the context, and a number of issues health IT operators such as clinical organisations, need to investigate during acquisition of health IT.

Keywords. Health IT safety, health IT procurement, health IT

Introduction

Adoption of IT in healthcare has offered new capabilities, while it has enhanced qualities of current capabilities, by offering increased processing power, storage, as well as automating mundane error-prone tasks. Adoption of health IT systems such electronic health records, picture archiving and communication systems, e-prescribing systems, as well as clinical decision support systems, have offered a number of advantages, including improvements in quality and safety of health services [1]. However, increasing reliance on IT may result in operational challenges, as even seemingly unimportant failures may have repercussions. For example, consider printers in a clinical organisation going offline for a limited period of time, and the impact of such an event on operations; in addition to the increased workload this may result in errors, with potential effect on the safety of the patients.

There are examples of many inconspicuous failures, which result in patient hazards, due to causes such as technical failures, badly designed user interfaces, mismatch between system interfaces and poor training. These reflect the fact that IT depended complex services constitute socio-technical systems [2]. Health IT operating organisations, need to include measures (assurances) that will provide confidence that these failures are controlled (e.g. use of paper based back up procedures, exhaustive testing of IT that will identify the majority of defects, comprehensive user training). When acquiring health IT, clinical organisations need to identify the strategy that will result in operating the contracted health IT with confidence.

[1] Corresponding Author. Email: g.despotou@warwick.ac.uk

1. What it means for a health IT operator to define critical requirements

In many critical industries, such as aerospace and energy, manufacturers and operators of computer systems, often have the onus to be in a position to convincingly demonstrate that their operation is fit-for-purpose. This involves gathering and explaining evidence through analysis and testing, that they have unintended use, and that these unintended conditions have been controlled to acceptable levels [3]. The operator of an IT system has ultimate responsibility for the safety and operational assurance of their services, as IT is an integral component of interdepending structures such as other systems, and people governed by a set of procedures and policies. Similarly, when contracting health IT, the operator (such as clinical organisations) will need to identify the aspects of its operation that may be critical to the safety and quality of the offered service **(**Figure 1**)**. Usually these can refer to unintended conditions such as failures, or wanted qualities (e.g., patient record not found, or patient images should be made available to clinicians within X time). These critical aspects will then be expressed as requirements during procurement of the health IT system (both examples represent real cases that have affected the safety of patients).

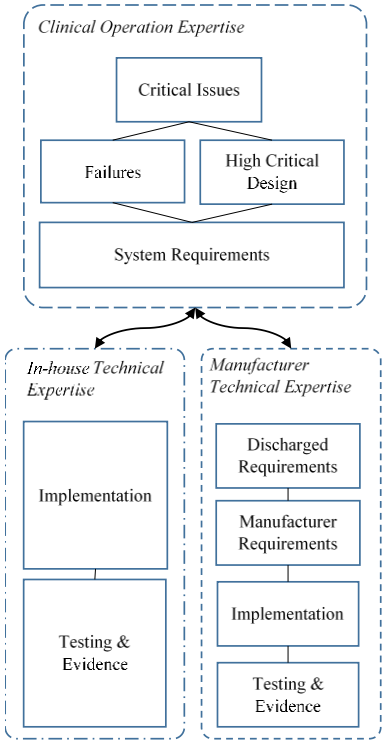

Figure 1. Operational and technical viewpoint dependencies

It is not uncommon for some of these requirements to be implemented by the clinical organisations' 'in-house' development team, offering a customised solution. In many cases, though, the organisation will contract the IT system from a manufacturer that will then assume responsibility in implementing the requirements discharged to them. In both cases, the respective development teams will need to produce the information necessary to support the requirements related to the critical aspects of the system's operation. This can include analysis, code walkthroughs, as well as white and black box testing, depending on the criticality of the service the system is contributing to. Furthermore, even if IT is developed in-house, it should be noted that IT developers may not be familiar with the operational needs of a system, for the expression of which, clinicians may be best suited. Separating the operational (what the system will do) from the technical (how it will be developed), allows separation of concerns and concentration of expertise at the right places. However, it is very important for an organisation to understand and manage these dependencies, as they can result in operational, safety, security, as well as business risks. Direct mismatch between requirements, as well as assumptions about these requirements will result in a system that does not correspond to the operational needs of an organisations. There are strategies helping to reduce the likelihood of these mismatches by identifying and documenting tacit knowledge; for example the UK ISB 0129 suggests a clinical advisor for IT manufacturers.

2. Auditing the manufacturer in order to increase confidence

An organisation that contracts an IT system needs to understand how their operational dependencies map on the manufacturer's development process and product in advance. Failure to do so may result in the operating organisation making assurance claims about the IT system, which eventually cannot be supported by the manufacturer. The following is a (non-exhaustive) list of issues that the authors consider may compromise the assurance efforts of the operator.

2.1. Compliance with standards and independent review

A manufacturer's compliance with standards will provide assurances that a known, trusted set of methods and processes has been used. However this does not guarantee the quality of the product of these processes, for which evidence gathered from testing will need to be provided. An operator can ask for a compliance statement and assessment, which in certain cases can be provided by an independent reviewer.

2.2. Training and support requirements

Training requirements can be underestimated, as there can be many implicit assumptions that if not true, may invalidate safety critical measures. For example, often issues raised from switching off alarms due to alarm fatigue, or overriding restrictions of the software may be attributed, in addition to poor design, to training or lack thereof. Furthermore, users of a system may need periodic training, or training after an update, in which case a more permanent agreement of support may offer benefits.

2.3. Field evidence and reporting

A manufacturer that has a structured reporting process is more likely to create a tracked operational record about their IT system. A clinical organisation may need to clarify if they have access to that data, also being notified in case an operator discovers a dormant issue with the system.

2.4. Adequacy, suitability and visibility of evidence and testing

An operator should not take the claims of a manufacturer about meeting the discharged to them requirements at face value. The operator should ask for a convincing but also suitable explanation. Compliance to standards, such as the CE mark and the Medical Device Directive (when applicable), as well as ISBs 0160 [5] and 0129 [4] in the UK, assists to this task. Standards stipulate techniques that experience has shown are suitable for certain problems. Furthermore, it should be noted that operators may prefer to explore options regarding visibility to the available evidence, rather than settle with a mere reference provided to it. However, if this is not an option, independent review and certification may warrant acceptance of appeal to a non-disclosed body of evidence.

2.5. Explanation of achievement of requirements

In many cases, there may be a logical leap between evidence, testing results and discharged requirements. Organisations, contracting IT systems, should consider asking for a documented explanation on how the testing results provide assurance that the requirements have been met, and under what specific assumptions.

2.6. Maintenance and update process

These are two very important issues, which may compromise the critical measures set in place by the operator. Maintenance and updates may affect the way a system is

configured or a function is provided, whilst the operator is unaware (particularly in automated software updates). Operators should ask for an update changelog and assess whether updates will affect the operational dependencies and assumptions.

2.7. Access to API and technical dependencies

Particularly for organisations that combine an IT system with in-house development, there may be a requirement to have access to the API, as well as access to other interface and knowledge of the technologies used.

2.8. Tacit knowledge extraction and customisation

Manufacturers should try to understand the operations of each organisation and how their IT relates to them; *they should not offer a fits-all solution*. Standards, such as the ISB 0129 [4], ask the manufacturer to involve a clinical expert in the process of procurement and customisation. Such experts will be able to elicit and elaborate on the justification of certain requirements, by providing a clear understanding how they are relevant to critical aspects of the system's operation in situ. Although this helps, clinical organisations have different procedures, thus a system that may be suitable for one may cause problems to another. The manufacturer should go through a structured process of eliciting this tacit operational information and suggest customisation to the operator. This can be very challenging, if not agreed during procurement, as any customisation of the system and its services may involve increased cost.

Conclusions

Health IT has become an integral part of many clinical services as it provides numerous benefits to organisations. An organisation procuring, contracting (even developing in-house), health IT systems needs to understand how the development can affect the confidence they can have in the operation of the health IT system. A number of issues need to be considered during procurement that might constitute business risks, which could result in overspending if realised late. The paper has presented issues, which can be used by clinical organisations, to audit the fitness of manufacturers to offer confidence in the safe operation of the health IT system about to be acquired. Although the list is non-exhaustive the authors have identified prominent issues based on their experiences; further work needs to result in a more comprehensive framework.

References

[1] Institute of Medicine, *Health IT and Patient Safety; building safer systems for better care, The National Academies Press, 2012*.

[2] Meeks D.W., Smith M.W., Taylor L., et al., *An analysis of electronic health record-related patient safety concerns*, J Am Med Inform Assoc 2014;21:1053-1059

[3] Despotou G., White S., Kelly T., Ryan M., *Introducing safety cases for health IT*, 4th international workshop on software engineering in healthcare p44-50, IEEE Press, 2012.

[4] ISB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems version 2, Maintained by the HSCIC.

[5] ISB 0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems version 2, Maintained by the HSCIC.