Data Safety Guidance for Clinical Risk Management

by Paul Hampton and Mark Thomas

Health organisations are increasingly using Health IT Systems in the provision of patient care. As with other sectors, the use of IT brings system safety risk and this in turn can have implications on patient safety. For example, if a system records patient allergies incorrectly, this could have dangerous if not fatal outcomes for patients if relied upon when administering medication. These risks have long been recognised by the industry and standards such as SCCI0129 and SCCI0160 have been established to inform the safety management systems of the manufacturers of Health IT System and those health organisations deploying such systems. As with other standards, however, risks associated with hardware and software is the main focus and there has been little or no explicit guidance on the management of safety data.

NHS Digital, in conjunction with the Safety-Critical Systems Club (SCSC) and the Data Safety Initiative Working Group (DSIWG), have therefore now published guidance - *Clinical Risk Management: Data Safety* - specifically to address the management of data in the clinical



healthcare context. This guidance is based on the work of the DSIWG, but has been tailored for the Healthcare context and specifically adapted to augment and complement the existing SCCI standards.

The guidance document is intended to be used in conjunction with the SCCI standards and aligns well to these, as the Data Safety Guidance (on which it is based) and the SCCI standard all follow a similar structure based around the established practices for the management of risk. The document is split into 3 broad sections:

- A general introduction to data safety;
- More detailed guidance on data safety aligned with the requirements of the SCCI standards;
- A structured methodology for assessing the risks.

Part 1: General Introduction to Data Safety

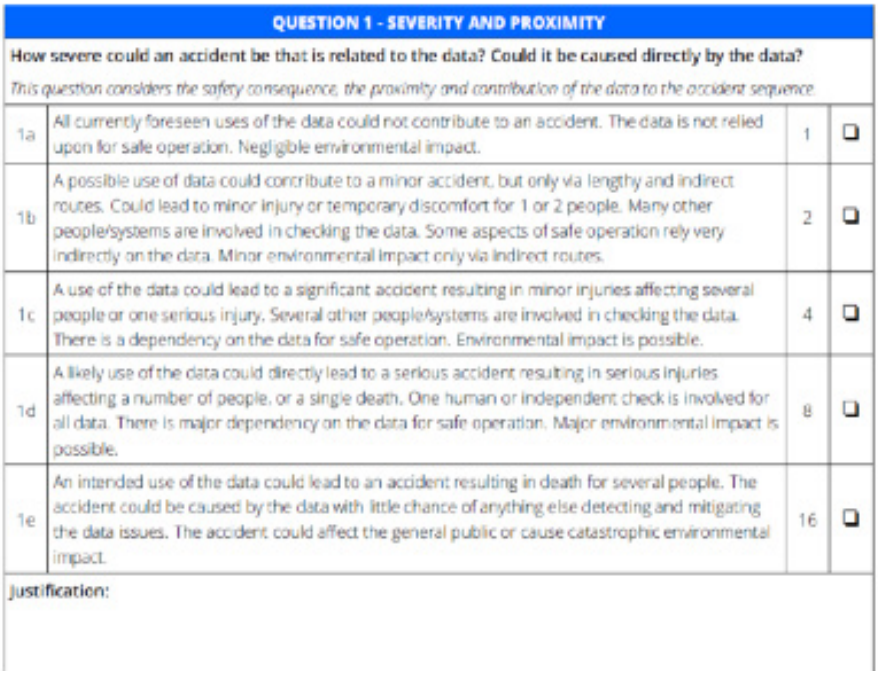
These sections provide an introduction to the subject, discuss the types and properties of safety data, the typical issues that can arise in healthcare settings, and provide a method for assessing the high-level applicability of data safety risks in an organisation.

These sections form an important part of the document as, irrespective of the remainder of the document, they play a significant role in raising awareness of the types of issue that data can give rise to, and as such, can help inform and educate those involved in the clinical risk management processes.

One early step in the risk management process is to establish the data safety context and to assess, at a high level, how much data safety is an issue for an organisation and the overall level of risk they

may be exposed to. This early assessment could then, for example, be used to help determine the scale of effort to invest in managing perceived data safety risks.

This assessment is conducted using an Operational Data Risk (ODR) assessment form. This is a tool developed by the DSIWG, and is structured as a questionnaire. Figure 1 shows an example screenshot from the tool. There are 8 questions in total, each covering different aspects of data safety that might typically contribute to risk assessment, for example: *How severe could an accident that is related to the data be? Could it be caused directly by the data?"* and *"What would be the impact on the organisation, client or public if an accident related to the data occurred?"* Answers are provided as a sliding scale of applicability with each option carrying a score. A total is then generated for all of the responses, and an overall ODR assessment level determined for the entire enterprise.



QUESTION 1 - SEVERITY AND PROXIMITY			
How severe could an accident be that is related to the data? Could it be caused directly by the data? *This question considers the safety consequence, the proximity and contribution of the data to the accident sequence*			
1a	All currently foreseen uses of the data could not contribute to an accident. The data is not relied upon for safe operation. Negligible environmental impact.	1	❑
1b	A possible use of data could contribute to a minor accident, but only via lengthy and indirect routes. Could lead to minor injury or temporary discomfort for 1 or 2 people. Many other people/systems are involved in checking the data. Some aspects of safe operation rely very indirectly on the data. Minor environmental impact only via indirect routes.	2	❑
1c	A use of the data could lead to a significant accident resulting in minor injuries affecting several people or one serious injury. Several other people/systems are involved in checking the data. There is a dependency on the data for safe operation. Environmental impact is possible.	4	❑
1d	A likely use of the data could directly lead to a serious accident resulting in serious injuries affecting a number of people, or a single death. One human or independent check is involved for all data. There is major dependency on the data for safe operation. Major environmental impact is possible.	8	❑
1e	An intended use of the data could lead to an accident resulting in death for several people. The accident could be caused by the data with little chance of anything else detecting and mitigating the data issues. The accident could affect the general public or cause catastrophic environmental impact.	16	❑
Justification:			

Figure 1: Organisational Data Risk Assessment Form

Part 2: Detailed Guidance on Data Safety Aligned with SCCI Standards

The SCCI standards are structured by defining requirements for each stage of the risk management process. The guidance sections provide, for each set of the standards' requirements, an interpretation of the requirement as it applies to data and the typical activities to consider when manging risks associated with data. These sections are described through the use of a worked example that describes a typical scenario where a manufacturer is providing a Health IT System to a health organisation who will be deploying it.

For example, the following requirements are defined in the SCCI standards:

SCCCI0129 Section 4.4.1: For each hazard identified the Maunfacturer MUST estimate, using the critieria specified in the Clinical Risk Management Plan:
- the severity of the hazard
- the likelihood of the hazard
- the resulting clinical risk.

SCCI0160 Section 4.4.1: For each identified hazard the Health Organisation MUST estimate, using the criteia specified in the Clinical Risk Management Plan:
- the severity of the hazard
- the likelihood of the hazard
- the resulting clinical risk.

The guidance document then goes on to describe a method for conducting hazard identification from a data perspective. This, for example, introduces the following dimensions to be considered when thinking about data hazards:

- Proximity: how directly a data failure will lead to an accident;
- Dependency: how dependent the application is on the dataset;
- Detection: the likelihood of being able to detect a data failure prior to an accident;

- Prevention: the ability ofthe system's architect/ developer to guard against errors;
- Correction: the ability of the system to work around or correct errors.

These can then be used in conjunction with a likelihood assessment to determine the overall data contribution to risk, as shown in Table 1 below. The likelihood calculated in this way, along with the assessed severity of the resulting impact, can then be used to determine the categorisation of the risk using a Clinical Risk Matrix, which will have been established as part of the risk assessment of hardware and the software hazard identification process.

We include a worked example to help illustrate the management of data safety using the guidance. The case study details are as follows:

A Manufacturer is building a new integrated health and social care system to support holistic care for community health services. The system supports clinical workflows for aspects such as referrals, tracking clinical encounters, appointment scheduling, outcome measures through to letter and report generation. The system follows a typical development lifecycle as a series of phases: business modelling, requirements, analysis and design, implementation, test and deployment. The system is being targeted to meet the requirements of a Health Organisation who are procuring a solution to help their cilinicians maintain a high level of quality of care

Concern	Very High/High	Medium	Low/Very Low
Proximity	A known use of the data is highly likely to lead to an accident	A possible use of the data could lead to an accident	All currently foreseen uses of the data could lead to harm only via lengthy and indirect routes
Dependency	Data is completely relied on	Data is indirectly relied upon	Little reliance on data
Detection	Low or no chance of anything else detecting an error	Some other people/systems are involved in checking the data	Many other people/systems are involved in checking the data
Prevention	Difficult or impossible to guard/barrier against errors	Possible to guard/ barrier against errors	Easy to guard/barrier against error
Correction	Difficult or impossible to correct or work around er-rors	Possible to correct or work around er-rors	Easy to correct or work around errors

Table 1: Data Hazard Risk Likelihood

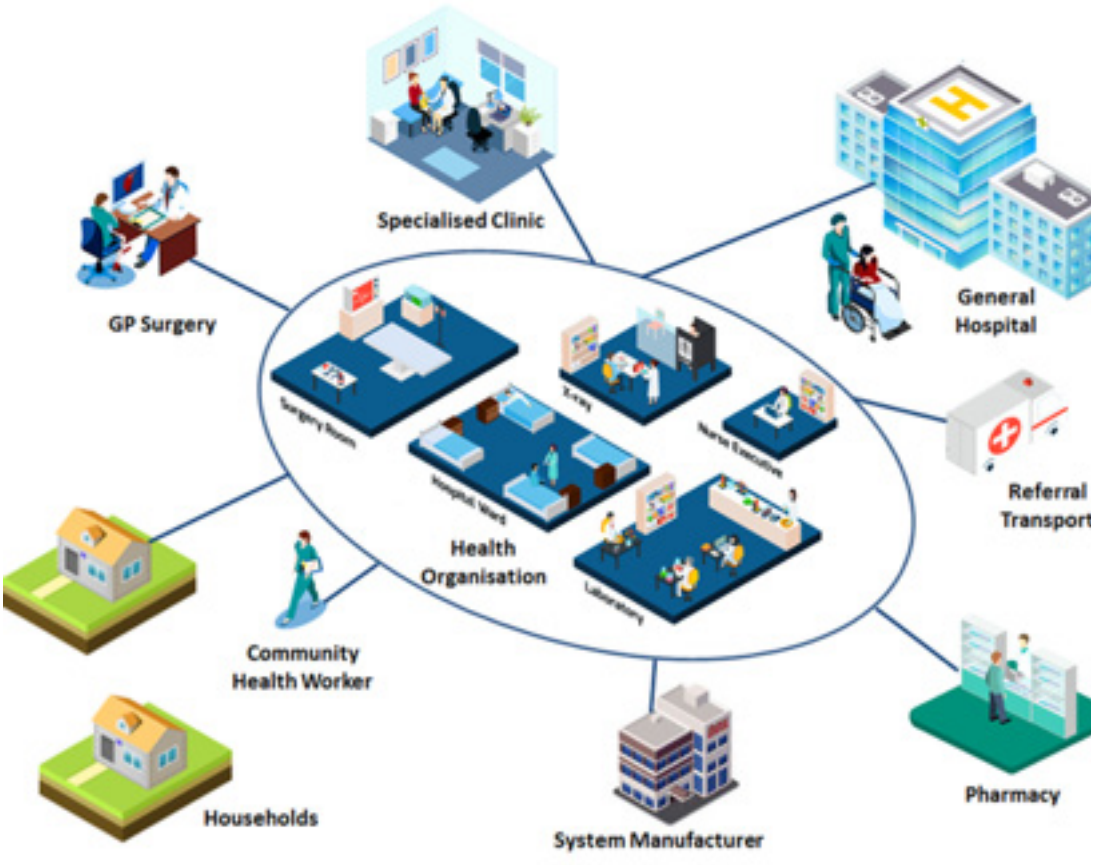


Figure 2: Case Study Scenario

in the face of increasing volumes of patients and pressure to reduce staff costs. The context for the integrated system is presented in Figure 2.

A Structured Methodology for Assessing Data Safety Risk

The final section in the guidance takes the form of an Appendix which provides a more formal, structured approach to the assessment of data safety risks and, inportantly, allows specific and appropriate 'good practice' risk management methods and techniques to be determined. We use the case study introduced above to illustrate the use of this methodology.

Use of the methodology is not mandated as part of the guidance, but it is highly recommended, since it allows linkage to be established between the idetified data safety risks and the good practice methods and techniques that are recommended to mitigate those risks.

The methodology uses the concept of Data Safety Assurance Levels (DSALS), which provide a more structured and systematic method of categorising risk. The DSALS are determined by extneding the risk assessment table already established in earlier sections, as indicated in Table 2.



Severity or Impact of data related accident	Very High / High	Medium	Low / Very Low
Catastrophic			
Multiple patient deaths. Permanent lifechanging incapacity and any condition for which the prognosis is death. Permanent lifechanging Incapacity for multiple patients. Severe injury or severe incapacity from which recovery is not expected in the short term for multiple patients.	DSAL4	DSAL4	DSAL3
Major			
A single death. Permanent lifechanging incapacity and any condition for which the prognosis is death for a single patient. Permanent lifechanging incapacity for a single patient. Severe injury or severe incapacity from which recovery is not expected in the short term for a single patient. Severe injury or severe incapacity from which recovery is expected in the short term for multiple patients. Severe psychological trauma for multiple patients.	DSAL4	DSAL3	DSAL2
Considerable			
Severe injury or severe incapacity from which recovery is expected in the short term for a single patient. Severe psychological trauma for a single patient. Minor injury or injuries from which recovery is not expected in the short term for several patients. Significant psychological trauma for multiple patients.	DSAL3	DSAL2	DSAL1
Significant			
Minor injury or injuries from which recovery is not expected in the short term for a single patient. Significant psychological trauma for a single patient. Minor injury from which recovery is expected in the short term for multiple patients. Minor psychological upset; inconvenience for multiple patients.	DSAL2	DSAL1	DSAL0
Minor			
Minor injury from which recovery is expected in the short term for a single patient. Minor psychological upset; inconvenience for a single patient.	DSAL1	DSAL0	DSAL0

Table 2: Data Safety Assurance Levels (DSALs)

Likelihood						
	Very High	DSAL1	DSAL2	DSAL3	DSAL4	DSAl4
	High	DSAL1	DSAL2	DSAL3	DSAL4	DSAL4
	Medium	DSAL0	DSAL1	DSAL2	DSAL3	DSAL4
	Low	DSAL0	DSAL0	DSAL1	DSAL2	DSAL3
	Very Low	DSAL0	DSAL0	DSAL1	DSAL2	DSAL3
		Minor	Significant	Considerable	Major	Catastrophic
		Severity				

Table 3: Clinical Risk Matrix

If a Clinical Risk Matrix is being used that is consistent with the matrix recommended in Section 4.4.3 of the Implementation Guidance to SCCI0129 and SCCI0160, then this table can be presented, as in Table 3 above.

Using this DSAL-oriented matrix simplifies the categorisation of data safety risk and allows recommended mitigations to be systematically determined.

Specific guidance on how data-related risks may be treated is presented in the Risk Treatment tables in Section 6.4 of the Data Safety Guidance, based on the data type and the DSAL of the data. These methods and techniques represent good practice in mitigating the risks associated with safety-related data. The Risk Treatment tables indicate where a particular method or approach is applicable to a given lifecycle data type and data property and, for each DSAL, whether the method/technique is recommended (R) or highly recommended (HR_. The lifecycle data types considered in the referenced version of the guidance are as follows:

- Verification (V);
- Infrastructure (I);
- Dynamic (D);
- Performance (P);
- Justification (J).

The applicable types of data property where the given technique could be effective in preserving that property are provided. These are coded to the 20 or so data properties identified, so for example 'I' indicates Integrity, 'C' Completeness, 'Y' Continuity etc..

Table 4 presents an example Risk Treatment table applicable to the case study example used in this paper.

It is expected that some interpretation may be required for these recommended techniques, depending on the nature of the system and the data, and indeed some may prove not to be applicable at all for certain applications. Nevertheless, it is recommended that each is given consideration, relevant interpretations are recorded and justification is provided where a technique is not adopted.

Conclusions

Health IT Systems are increasingly dependent on data and when issues arise with that data, there are risks to patient safety with potentially the same severity of impact as those normally associated with accidents caused by software or hardware. Management of data safety risks has not historically been addressed in safety standards; standards do exist, but these are primarily focussed on software and hardware. NHS Digital guidance has now been developed in conjunction with the Safety-Critical Systems Club and the Data Safety Initiative Working Group; this has been tailored to the Healthcare domain and supplements the existing Healthcare Standards. This guidance describes practices, methods and techniques that represents good practice in the

6.4.2.3 System Design

Technique	Data Types	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
Built-in-Test / Built-in-Test Equipment (BIT / BITE)	..D..	-	R	HR	HR	Application tests the data (e.g., at start-up or when requested by an operator).	IC.....V.....
Cyclic / Continuous BIT	..D..	-	-	R	HR	Application applies tests to the data it is processing continuously (e.g., for a live data stream) or periodically (e.g., every nth message, every hour).	IC.Y.....VL.....
Backward recovery	..D..	R	R	HR	HR	If a fault in data has been detected, the system resets to an earlier internal data set, which has been proven consistent.	IC.....
Parity Checks	..D..	R	R	HR	HR	Within data, e.g., Hamming codes, Reed-Solomon, Hagelbarger.	I.....
Automatic Error Correction	..D..	R	R	HR	HR	Detected errors are corrected automatically.	IC.....
Checksums / Cyclic Redundancy Checks (CRCs) / Hashes	..D..	-	R	HR	HR	Digests of data sets are produced, included with the data set and checked to provide confidence that the data is unaltered.	IC.....
Digital Signatures	..D..	-	R	HR	HR	For non-repudiation and integrity of data.	I.....T.....U.....
Sequence Numbers	..D..	R	R	HR	HR	Data bears sequence numbers so the integrity of a data stream can be checked (e.g., monotonic increase, duplicate detection).	ICN.....PQ.....
Automatic Repeat Request	..D..	R	R	HR	HR	Automatic Repeat-reQuest (ARQ) to repeat transmission of data which has not been received correctly.	IC.Y.....

Table 4: Example Risk Treatment Table

management of safety risks associated with data.

Paul Hampson *is a Chartered Engineer with over 28 years' experience in IT. He spent 15 years designing and developing enterprise systems in sectors including energy & health. He has extensive and varied systems safety experience, including corporate governance and assurance, and healthcarse standards-based safety engineering.*

Mark Thomas *is a safety engineer with 30 years' experience in the defence, nuclear and health sectors. He holds full memberships with the IET and the IMA and represents the UK via the BSI on the international committee responsible for developing an update to ISO80001. Mark holds degrees in Mathematics from the OU and LMU..*