Assuring Patient Safety in Relation to E-Health Systems and Applications. A Professional Practice Standard

Part B: The Standard

Edited by
David Rowlands
Dr John Zelcer
Dr Trish Williams
# Table of Contents

1. Preface ........................................................................................................................................... 3
2. Acknowledgments .......................................................................................................................... 4
3. Purpose ........................................................................................................................................... 5
4. Acronyms ......................................................................................................................................... 6
5. Definitions ....................................................................................................................................... 7
6. Introduction ..................................................................................................................................... 13
   6.1 What the Standard Is .................................................................................................................. 13
   6.2 Who the Standard is Used by ....................................................................................................... 14
   6.3 How the Standard was Developed ............................................................................................. 15
       6.3.1 Ongoing Maintenance ........................................................................................................ 16
   6.4 Overview of the Standard ........................................................................................................... 16
7. Ethical Practice ............................................................................................................................. 17
9. Stakeholders ..................................................................................................................................... 25
10. Summary of Requirements ........................................................................................................... 29
11. Incorporating Patient Safety into Enterprise Governance ............................................................ 33
12. Undertake Patient Safety Risk Assessment .................................................................................... 39
13. Manage Patient Safety Across the E-Health System Lifecycle ......................................................... 42
   13.1 Define the Problem .................................................................................................................... 45
   13.2 Planning for Solution(s) ........................................................................................................... 48
   13.3 Obtaining Solution(s) .............................................................................................................. 51
   13.4 Implementation ....................................................................................................................... 55
   13.5 Operation and Maintenance of E-Health Systems and Applications ....................................... 57
   13.6 Decommissioning and Disposal ............................................................................................... 61
14. Measure and Provide Feedback on Patient Safety ........................................................................... 63
15. Documentation ............................................................................................................................... 67
   15.1 Safety Program Documentation ................................................................................................. 67
   15.2 Risk Register(s) ....................................................................................................................... 68
   15.3 Safety Case ............................................................................................................................. 68
16. References ....................................................................................................................................... 69
17. Version Control ............................................................................................................................... 71
List of Tables

Table 1. Summary of Requirements in the Standard ............................................. 29

List of Figures

Figure 1 - Conceptual Framework for Patient Safety in Relation to E-Health......................... 22
Figure 2 – Patient-safety Stakeholder Map........................................................................ 26
Figure 3 - E-Health System / Application Life Cycle Model ............................................. 43
PART B: The Standard

Assuring Patient Safety in Relation to E-Health Systems and Applications
1. Preface

The HISA Board of Directors is pleased to introduce this professional practice standard Assuring Patient Safety in Relation to E-Health Systems and Applications. A Professional Practice Standard. Part B: The Standard. This document is to be read in conjunction with Part A: Information Paper.

This current version of the document is a draft, released for public comment to HISA members and stakeholders. All comments received will be reviewed by the editors and will influence the final edition.

This professional practice standard is the first publication of this work. All the contributors are experienced professionals who understand the need for e-health to be designed, implemented and used appropriately. They also understand the important role health informaticians play in the design, implementation and use of e-health systems.

HISA is grateful for the work of the editors and expert advisory committee who have developed a thorough and valuable resource for organisations and individuals involved with the design and implementation of information technology products and services for e-health.

2015 – 2016 HISA Board of Directors
HISA: Health Informatics Society of Australia Ltd
## Acknowledgments

<table>
<thead>
<tr>
<th>E-Safety Expert Group</th>
<th>Other Contributors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rodney Ecclestone</td>
<td>Don Newsham</td>
</tr>
<tr>
<td>Neville Board</td>
<td>Neil Gardner</td>
</tr>
<tr>
<td>Dr Vince McCauley</td>
<td>Dr David Hansen</td>
</tr>
<tr>
<td>Dr Michael Legg</td>
<td></td>
</tr>
<tr>
<td>Prof Nilmini Wickramasinghe</td>
<td></td>
</tr>
<tr>
<td>Lyn David</td>
<td></td>
</tr>
<tr>
<td>A/Prof Meredith Makeham</td>
<td></td>
</tr>
<tr>
<td>Antonio Abbenante</td>
<td></td>
</tr>
<tr>
<td>Dr Damian Claydon-Platt</td>
<td></td>
</tr>
<tr>
<td>Dr Bob Webb</td>
<td></td>
</tr>
<tr>
<td>Michelle Alcock</td>
<td></td>
</tr>
<tr>
<td>Nigel Chartres</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

When designed, implemented and used appropriately, e-health can be a positive enabler of safety, quality, effectiveness and productivity in health care delivery. However, some concerns about harm associated with the use of e-health systems and applications have emerged both in Australia and internationally, as the technologies concerned are increasingly complex and operate in complex socio-technical environments. Accordingly, there is potential for unintended or unexpected consequences.

This Professional Practice Standard is the second of a three part series on assuring patient safety in the implementation of e-health. The three parts are:

- **Part A: Information Paper.** Designed to accompany the standard, the Information Paper provides an overview of the topic and establishes the rationale for the standard.

- **Part B: Professional Practice Standard** (this document). This Standard sets out a range of requirements for both organisations and individual health informaticians involved with information technology products and services for e-health.

- **Part C: Supporting Resources.** Part C provides a substantial set of tools and information for implementers of the standard as well as providing guidance concerning compliance with it.

In addition, an online training course will be developed to assist implementers of the standard and to inform other parties who want to know more about the topic.

The specific objectives of this professional practice standard are to ensure that:

- Potential hazards associated with clinical information systems are prospectively identified throughout the system life cycle and that potential risks are mitigated.

- Hazardous situations that do eventuate are quickly identified and associated harm is minimised.

- The health and e-health supply industries systemically improve Australian e-safety.
## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSQHC</td>
<td>Australian Commission on Safety and Quality in Health Care</td>
</tr>
<tr>
<td>AIIA</td>
<td>Australian Information Industries Association</td>
</tr>
<tr>
<td>HISA</td>
<td>Health Informatics Society of Australia</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>MSIA</td>
<td>Medical Software Industry Association</td>
</tr>
<tr>
<td>WHO</td>
<td>World Health Organization</td>
</tr>
</tbody>
</table>
### Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acceptance testing</strong></td>
<td>Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system.</td>
</tr>
<tr>
<td><strong>Accountable</strong></td>
<td>Being held responsible.</td>
</tr>
<tr>
<td><strong>Actions taken to reduce risk</strong></td>
<td>Actions taken to reduce, manage or control any future harm, or probability of harm, associated with an incident.</td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td>A substance, object or system which acts to produce change.</td>
</tr>
<tr>
<td><strong>Clinical</strong></td>
<td>Relating to or based on work done with patients/clients.</td>
</tr>
<tr>
<td><strong>Clinical Incident</strong></td>
<td>See patient safety incident</td>
</tr>
<tr>
<td><strong>Clinical information system</strong></td>
<td>A system that deals with the collection, storage, retrieval, communication and use of health related data, information and knowledge pertaining to patients.</td>
</tr>
<tr>
<td><strong>Clinical workflow</strong></td>
<td>The who, what, where, when, how and why things get done in clinical practice.</td>
</tr>
<tr>
<td><strong>Clinician</strong></td>
<td>A health professional registered with the Australian Health Practitioner Regulation Agency (AHPRA).</td>
</tr>
</tbody>
</table>
Clinician Engagement: The manner in which clinicians are involved in planning, delivery, use, improvement and evaluation of clinical IT.

Control: The means of guiding a system (making decisions and both enabling and constraining activities).

Disability: Any type of impairment of body structure or function, activity limitation and/or restriction of participation in society, associated with past or present harm.

(Source: World Health Organization, 2009)

Disease: A physiological or psychological dysfunction.

(Source: World Health Organization, 2009)

E-health: The use of health information technologies to provide health care services.

E-iatrogenesis: A state of affairs in which patient harm is caused at least in part by the application of clinical information systems.

Enabling technology: Equipment and/or methodology that, alone or in combination with associated technologies, provides the means to generate giant leaps in performance and capabilities of the user.

(Source: BusinessDictionary.com)

E-safety culture: The product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation’s management of e-safety.

(Source: based on HSC, 1993)

Event: Something that happens to or involves a patient.

(Source: World Health Organization, 2009)

Fitness for purpose: Ability to perform the task it was designed to do.

Functional testing: Testing based on an analysis of the specification of the functionality of a component or system.

(Source: International Software Testing Qualifications Board, 2014)

Harm: Harm: impairment of structure or function of the body or mind and/or any deleterious effect arising there from. Harm includes disease, injury, suffering, disability and death.

(Source: World Health Organization, 2009)

Harmful incident (adverse event): An incident which resulted in harm to a patient.

(Source: World Health Organization, 2009)
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hazard</strong></td>
<td>A circumstance, agent or action with the potential to cause harm.</td>
<td>(Source: World Health Organization, 2009)</td>
</tr>
<tr>
<td><strong>Health</strong></td>
<td>A state of complete physical, mental and social wellbeing and not merely the absence of disease or infirmity.</td>
<td>(Source: World Health Organization, 2009)</td>
</tr>
<tr>
<td><strong>Healthcare</strong></td>
<td>Services received by individuals or communities to promote, maintain, monitor or restore health.</td>
<td>(Source: World Health Organization, 2009)</td>
</tr>
<tr>
<td><strong>Healthcare-associated harm</strong></td>
<td>Harm arising from or associated with plans or actions taken during the provision of healthcare, rather than an underlying disease or injury.</td>
<td>(Source: World Health Organization, 2009)</td>
</tr>
<tr>
<td><strong>Health informatician</strong></td>
<td>A professional in the science and practice around information in health that leads to informed and assisted health care, who is involved with clinical information systems.</td>
<td>(Source: based on HISA, not dated)</td>
</tr>
<tr>
<td><strong>Implementer</strong></td>
<td>A person or organisation who/which is responsible for the deployment of a health information system,</td>
<td></td>
</tr>
<tr>
<td><strong>Integration testing</strong></td>
<td>Testing performed to expose defects in the interfaces and in the interactions between integrated components or systems.</td>
<td>(Source: International Software Testing Qualifications Board, 2014)</td>
</tr>
<tr>
<td><strong>Injury</strong></td>
<td>Damage to tissues caused by an agent or event.</td>
<td>(Source: World Health Organization, 2009)</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Continual checking, supervising, critically observing or determining status in order to identify change from the performance level required or expected.</td>
<td>(Source: Standards Australia, 2009)</td>
</tr>
<tr>
<td><strong>Near miss</strong></td>
<td>An incident which did not reach the patient.</td>
<td>(Source: World Health Organization, 2009)</td>
</tr>
<tr>
<td><strong>Organisation</strong></td>
<td>An entity that is involved with a clinical information system or systems. This includes but is not limited to designers and developers, implementers, operators/users, maintainers, and expert advisers.</td>
<td></td>
</tr>
</tbody>
</table>
Patient

A person who is a recipient of healthcare.

(Source: World Health Organization, 2009)

Note: Synonyms for ‘patient’ include consumer and client.

(Source: ACSQHC, 2012)

Patient safety

The reduction of risk of avoidable harm associated with healthcare to an acceptable minimum.

(Source: World Health Organization, 2009)

Patient safety incident

An event or circumstance which could have resulted, or did result, in harm to a patient.

(Source: World Health Organization, 2009)

Preventable

Accepted by the community as avoidable in the particular set of circumstances.

(Source: World Health Organization, 2009)

Residual risk

The risk remaining after controls are taken into account.

(Source: Standards Australia, 2009)

Review

Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

(Source: Standards Australia, 2009)

Risk

The effect of uncertainty on objectives, expressed as the combination of the probability of occurrence of harm and the severity of that harm.

(Source: Standards Australia, 2009)

Risk acceptance

The acceptance of a risk, as a residual risk or without mitigation, where the severity of a risk is lower than the risk tolerance, and the added cost to avoid the risk is not justified.

(Source: Whitman & Mattord, 2009)

Risk assessment

The overall process of risk identification, risk analysis and risk evaluation.

(Source: Standards Australia, 2009)

Risk appetite

The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission or vision.

(Source: ISACA, 2009)

Risk tolerance

The acceptable variation relative to the achievement of an objective.

(Source: ISACA, 2009)
| **Safety** | The reduction of risk of unnecessary harm to an acceptable minimum.  
*Source: World Health Organization, 2009* |
| **Safety critical function** | Any function whose failure may result in significant harm. |
| **Safety case** | Documentation which confirms that the development, deployment and use of clinical IT will not pose an unacceptable level of safety risk.  
*Source: Based on COACH eSafety Guidelines, 2013* |
| **Stakeholder** | A person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.  
*Source: Standards Australia, 2009* |
| **Suffering** | The experience of anything subjectively unpleasant.  
*Source: World Health Organization, 2009* |
| **System testing** | The process of testing an integrated system to verify that it meets specified requirements.  
*Source: International Software Testing Qualifications Board, 2014* |
| **Unit (component) testing** | The testing of individual software components.  
*Source: International Software Testing Qualifications Board, 2014* |
| **Usability testing** | Testing to determine the extent to which the software product is understood, easy to learn, easy to operate and attractive to the users under specified conditions that facilitate safe operation.  
*Source: International Software Testing Qualifications Board, 2014* |
2. Introduction

Information technologies now play a major role in the delivery of health care, and this will continue to increase. A wide range of e-health systems and applications provide essential record keeping and logistical support, analyse clinical data, apply clinical knowledge and assist clinicians with in-situ decision making. Health applications routinely take clinical and other health-related measurements and guide clinical actions, and the “internet of things” pervades health behaviours.

The World Health Organization (WHO) defines patient safety as the reduction of risk of unnecessary harm associated with healthcare to an acceptable minimum. An acceptable minimum refers to the collective notions of given current knowledge, resources available and the context in which care was delivered weighed against the risk of non-treatment or other treatment.

This Professional Practice Standard and its supporting resources aim to promote patient safety specifically in relation to e-health; and by doing so improve health care delivery in Australia.

2.1 What the Standard Is

This Professional Practice Standard (Standard) establishes a set of requirements for a systematic approach to the achievement of patient safety in relation to e-health, against which the performance of organisations can be assessed and which individual health informaticians identify their duties of care.

The Standard is capability oriented. It articulates a set of requirements - expectations of the existence of capabilities - which collectively provide evidence of a systematic approach. These requirements are expressed as either:

- “Shall”, indicating that conformance to the requirement is mandatory for organisations and/or individuals who choose to adopt the standard.
- “Should”, indicating that conformance is desirable for organisations and/or individuals who choose to adopt the standard.

The means of satisfying these requirements will differ from organisation to organisation and informatician to informatician, taking into account varying objectives, needs, contexts, structures, cultures and other factors. Part C, Supporting
Resources, will provide and reference a range of methods, tools and background
Resources, assimilates knowledge to assist with implementation of the Standard, and
is intended to be informative rather than prescriptive (normative).

This Standard is designed to meet the needs of:

- Staff and/or agents of organisations who are accountable for achieving patient
  safety.
- Staff and/or agents of organisations who implement, operate or maintain e-
  health systems and applications.
- Staff and/or agents of organisations who are responsible for establishing and
  maintaining corporate and clinical governance.
- Developers of e-health systems and applications and their enabling technologies.
- People and organisations that audit and/or evaluate performance in achieving
  patient safety.
- Developers of related standards and guidelines.

2.2 Who the Standard is Used by

Clinical practice requires highly reliable organisational support in order to assure
safety. The characteristics of high reliability organisations, not just in health care but
also in a range of other safety critical industries, include the use of systematic,
evidence-based approaches, “collective mindfulness” and reference to experts¹.

Accordingly, this Standard may be applied either:

- To organisations which are involved with e-health and which are striving to
  achieve demonstrable levels of professional practice in relation to patient safety.

Examples of organisations that are involved with e-health include:

- Healthcare organisations using or intending to use information technology
  products and services for clinical purposes (e.g. clinical records, decision
  support, ordering), at any point in the system life cycle from conception to
  disposal.
- Clinical software developers, suppliers and implementers.

¹ For example: “High-reliability organizations (HROs) stay safe ... [through] ... an environment of “collective
mindfulness” in which all workers look for, and report, small problems or unsafe conditions before they pose a
substantial risk to the organization and when they are easy to fix”; and “[high reliability organisations (HROs)]
enhance their resilience by ... deference to expertise. When confronted by a new threat, HROs have mechanisms
in place to identify the individuals with the greatest expertise relevant to managing the new situation and to place
decision-making authority in the hands of that person or group. They do not invoke organizational hierarchy or
expect that the person with the most seniority or highest rank will be the most effective at dealing with the
problem“. (Chassin & Loeb, 2013).
Professional service organisations advising on the usage and acquisition of e-health.

- To individual health informaticians involved with e-health and striving to achieve a demonstrable level of professional practice in relation to patient safety, irrespective of whether their organisation adopts the standard.

Health informaticians may be working in any of the example organisations above.

Both organisations and informaticians have duties of care to deliver safe e-health products, services and practices. This Standard articulates specific requirements for these duties of care.

### 2.3 How the Standard was Developed

This Professional Practice Standard is currently in draft form only, for the purposes of broad consultation. It has been developed by expert volunteers for the Health Informatics Society of Australia (HISA), with wide stakeholder consultation using the following processes.

Initial discussion drafts of the Standard, the associated information paper and supporting resources were developed by a HISA volunteer drafting group and reviewed by a HISA expert volunteer review group. In June 2015 the HISA Board endorsed the use of these drafts for the first stages of consultation and communication.

Two workshops were undertaken in association with HIC2015:

1. A 90 minute session open to any HIC attendee, in which the need for and development of the standard was communicated.
2. A workshop for invited experts, in which the content of the Standard was reviewed in detail and plans for their progression formulated.

Following these workshops, the Standard was updated and reviewed by the HISA volunteers. It was then provided to experts at the International Organization for Standardization (ISO) for external review, and minor modifications ensued.

In February 2016 the HISA Board endorsed this draft Standard for the purposes of public consultation. The Standard will be further iterated taking into account feedback received from consultation processes.

---

2 Australia's premier digital health, e-health & health informatics conference, held in Brisbane in August 2015.
2.3.1 Ongoing Maintenance

The Standard will be reviewed and updated as required on a two-yearly basis, following its finalisation.

2.4 Overview of the Standard

The Standard establishes a set of ethics with respect to clinical information system related patient safety. Drawing from these ethics, a conceptual framework for establishing a systematic approach is articulated.

A set of requirements, categorised in terms of the conceptual framework, is then presented. Each requirement takes the form of a statement of expectations of the existence of a specific capability; and one or more descriptors elaborating the requirement.
3. Ethical Practice

Elements of ethical practice in relation to patient safety associated with e-health reflect fundamental principles of ethics. Many of these are in common with those adopted in medical/clinical ethics and can be seen to be at healthy tension with one another in key clinical decision making environments. These principles include but are not limited to concepts of autonomy, non-maleficence, beneficence, consequentialism, paternalism and utilitarianism.

Elements of ethical practice in relation to e-health include:

1. E-health systems are used directly in clinical practice. Accordingly, patient safety must be a primary consideration in their design, development, implementation, operation, maintenance and disposal of such systems.

   Implications include:
   - All organisations and individuals associated with e-health, in any capacity, must commit to patient safety as a fundamental outcome.
   - All organisations and individuals associated with e-health, in any capacity, must put in place measures to assure patient safety.

2. Achievement and maintenance of patient safety is a duty of care for organisations and individuals involved with e-health.

   Implications include:
   - Individuals involved with e-health must take personal responsibility for patient safety.
   - Organisations and individuals must maintain awareness of legal and other regulatory requirements and the ways in which compliance is met and assessed.

3. Patient safety in relation to e-health requires ongoing vigilance from everyone involved; and commitment to act where hazards are identified or patient safety incidents occur.

   Implications include:
• Organisations and individuals have the responsibility to initiate action where hazards are identified. This includes health informaticians escalating perceived hazards in their organisations as required.

• Organisations have the responsibility to consider all patient safety related issues and act accordingly.

4. **Patient safety in relation to e-health requires the coherent, systematic, structured and timely application of controls.**

Implications include:

• Coherence – patient safety controls in relation to e-health must be capable of integrating/interoperating with other relevant management frameworks used in healthcare and ICT, such as risk management, quality management, other dimensions of patient safety and clinical governance.

• Systematic – patient safety controls in relation to e-health must be guided by consistent policies, processes, structures and evidence-based methodologies that can be applied methodically and replicated.

• Structured – patient safety controls in relation to e-health must be clearly articulated across the organisation and use definitive patterns that enable common understanding between disparate stakeholders.

• Timely – patient safety controls in relation to e-health must be able to capture feedback and enable interventions within timeframes appropriate to the levels of risk involved.

5. **The achievement and maintenance of patient safety in relation to e-health must be based on the best available evidence.**

Implications include:

• Approaches used to pursue patient safety in relation to e-health should be based, where reasonably possible, on research that is: demonstrably relevant; can be translated into practice; and is based on sound methodology.

• Systematic approaches should be used to apply evidence. A generic process, consistent with methodologies used in the application of evidence-based clinical practice, is: frame the question; find the evidence; assess the evidence; apply the evidence; evaluate the outcomes.

• Some inputs to the achievement and maintenance of patient safety are likely to be based on sources such as historical data, experience, stakeholder feedback, observation, forecasts, modelling and expert judgement, particularly where “cutting edge” technologies are implemented.
Accordingly, decision makers should take into account any limitations of evidence and the possibility of divergence among experts.

6. **Achievement and maintenance of patient safety in relation to e-health must be based on open and transparent processes.**

Implications include:

- Ensuring that stakeholder input is welcomed. Different stakeholders are likely to have differing perspectives and capabilities, and harvesting these effectively can lead to more robust approaches to improving patient safety.

- Openness and transparency have implications for:
  - Resourcing – open and transparent processes may add costs to the organisation, however this should not be confused with economic benefit. A more costly process may be economically beneficial if patient safety is achieved as a result and the costs of dealing with patient safety failures are avoided.
  - Timing - open and transparent processes may take longer. However, this should be built into expectations and is likely to be time well spent, as with cost vs economic benefit.

[Note: commercial confidentialities will at times impinge on openness and transparency. However, tensions such as these should be openly discussed between contracting parties and viable approaches to maximizing openness and transparency negotiated.]

7. **Patient safety incidents arising from the use of e-health should be treated in the same way that other such incidents should be treated in clinical practice.**

Implications include:

- Organisations should build awareness and understanding of patient safety in relation to e-health in their workforces.
- Organisations should cross-reference to relevant professionally based clinical governance guidelines, for example as promulgated by clinical colleges.
- Organisations should capture and continuously improve data, information and knowledge supporting safer health care.
- Organisations should support those who work in the health system to deliver safer patient care.
- The Australian Open Disclosure Framework (for harmful incidents) should be applied (ACSQHC, 2003).
4. Conceptual Framework for Patient Safety in Relation to E-Health Systems and Applications

The Australian Safety and Quality Framework for Health Care (ACSQHC, 2010) specifies three core principles for safe and high-quality care. These are that safe, high-quality health care is always: consumer-centred; driven by information; and organised for safety. The implicit message from the Commission is that safe, high quality care happens by design, rather than being organic.

Patient safety in relation to e-health represents a specific sub-domain of patient safety in healthcare.

Achievement and maintenance of patient safety in relation to e-health is dependent on the effectiveness of the management frameworks that organisations and individuals use. It is too complex and too important to rely on ad hoc measures. Effective frameworks describe the domain and provide the foundations upon which structures, processes, policies and other control mechanisms can be built into a coherent set of capabilities.

The conceptual framework below provides the structure for this Standard, defining its scope and constituent elements.
Figure 1 - Conceptual Framework for Patient Safety in Relation to E-health

This conceptual framework embraces and builds upon one of the core principles from the Australian Safety and Quality Framework for Health Care (ACSQHC, 2010) – organising for safety.

The ACSQHC document describes areas for action that all people in the health system can take to improve the safety and quality of Australian healthcare. Being organised for patient safety specifically includes:

- All stakeholders having a role in patient safety and preventing or minimising harm arising from healthcare.
- Supporting, implementing and evaluating clinical information systems.

While the scope of the ACSQHC document is the health system, it is entirely reasonable to expect or indeed demand that others involved in clinical information supply chains, such as health software suppliers, information and knowledge intermediaries and expert advisers, to also be organised for safety.

Building on this organisation for safety, the conceptual framework comprises the following components:

- Incorporation of patient safety into enterprise governance. This embraces two major points. First, it affirms that governance, embracing both corporate and clinical dimensions, is critical to a systematic approach. Second, “incorporation” suggests that patient safety should work with, and if appropriate within, other dimensions of enterprise governance rather than standing alone.
- Undertaking risk assessment. The definition of patient safety is based on the concept of risk, so risk assessment is a central platform.
• Managing patient safety across the system lifecycle. E-health systems and applications need to be safe from conception to retirement, so the system lifecycle is an important construct. It forms the organising framework for risk treatment and establishing other controls.

• Measurement and feedback. Effective control systems, by definition, use feedback for ensuring the appropriateness, effectiveness and efficiency of controls; and evidence-based control systems have a responsibility to contribute to building the evidence base, learning from cases and incidents to modify system behavior and outcomes.

• The final component of the framework is documentary deliverables. Again, this standard does not seek to prescribe the form of or processes for developing relevant documentation. However, the minimal documentation requirements articulated are common to all such management frameworks, and comprise:
  1. A documented patient safety program, detailing sufficient details about the approach taken and initiatives planned or implemented to enable: effective governance; recognition of success and failure; and stakeholder communication and alignment.
  2. A risk register – a basis for monitoring and managing identified risks.
  3. A safety case, documenting controls implemented and their performance as well as program outcomes; building the evidence base; and enabling accountability.
  4. Incident and near miss reporting.

It is important to note that these documents need not be stand-alone. For example, the risk register for patient safety in relation to clinical information systems may be a component of a larger risk register.

Examples of these documents are included in Part C, Supporting Resources.
5. Stakeholders

The potential range of stakeholders in patient safety in relation to e-health is as wide as the range of stakeholders in health.

Stakeholders are “mapped”, for the purposes of this Standard, according to their adjacency to the center of e-iatrogenesis. At the centre are stakeholders who have the potential to be harmed. Stakeholders further from the centre may suffer consequences in association with e-safety (e.g. financial or reputational damage), or may be contributors to patient safety.

At the centre of the stakeholder map depicted at Figure 3 below are patients and clinicians – the parties directly involved in clinical care:

The next layer of stakeholders is health service organisations, within and between which clinical care is delivered. This specifically includes those responsible for:

- Overall (executive) governance – those who are ultimately responsible for ensuring effective patient safety governance and capability.
- Clinical governance – the system through which the safety quality of patient care is maintained and improved.
- IS/IT governance – the system through which the safety and quality of clinical information systems is maintained and improved.
- Quality and safety governance - the system through which the quality and safety of the health service as a whole is maintained and improved.
- Health informaticians are identified here as a distinct group of stakeholders. In practice, health informaticians engaged in clinical information systems will generally fall into one or more of the categories already described. However, as people who are expected to have competence across the array of areas relevant to clinical information systems, health informaticians have heightened responsibilities for patient safety in this domain.
The next layer of e-safety stakeholders is clinical IT product and service suppliers. These include:

- E-health system designers and developers. Ensuring patient safety requires understanding and applying the most effective development methods.

- Vendors. The vendor community has a central role in understanding and responding to patient safety issues, providing information transparently about safety concerns that may arise from products they sell, and working closely with healthcare organisations that buy their systems to ensure safe implementation and operation.

- Clinical information and knowledge suppliers. Clinical information and knowledge provided via e-health systems are often sourced from third party suppliers or intermediaries.
• System integrators and implementers. A range of integration, configuration and implementation services may be involved in customising and deploying e-health systems including project and change managers, interface specialists, integration architects and trainers.

• Other advisors, for example professional service providers. Patient safety needs to be incorporated into all organisational strategies associated with e-health systems and applications.

There are also several other groups of stakeholders that may either currently or potentially be involved with patient safety in relation to e-health:

• Influencers include health IS/IT policy makers (including the Australian Commission on Safety and Quality in Health Care (ACSQHC) and other Australian, State and Territory Governments); professional and industry bodies (including HISA, the Medical Software Industry Association (MSIA) and the Australian Information Industries Association (AIIA)); health informatics educators and trainers; and researchers interested in patient safety.

• Potential stakeholders who are currently involved with patient safety, including: regulators, standards developers (e.g. ISO TC215, HL7 International); and certifiers and accreditors of both e-health systems and health service delivery.

A responsibility assignment matrix for these roles is included in Part C, Supporting Resources.
6. **Summary of Requirements**

The following table uses the framework presented at Figure 2 to categorise the requirements of this Standard. The requirements are elaborated in sections 6 – 9.

Many of the standards are simply part of processes that organisations and health informaticians should be doing anyway, but are recognised in the available literature as being of particular importance to e-safety.

**Table 1. Summary of Requirements in the Standard**

<table>
<thead>
<tr>
<th>Requirements for Patient Safety in Relation to E-health Systems and Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incorporate Patient Safety into Enterprise Governance</strong></td>
</tr>
<tr>
<td>2. Document programs.</td>
</tr>
<tr>
<td>3. Appoint responsible officer(s).</td>
</tr>
<tr>
<td>5. Clinician engagement.</td>
</tr>
<tr>
<td>6. Promote cultures conducive to patient safety.</td>
</tr>
<tr>
<td>7. Communicate and consult with stakeholders.</td>
</tr>
<tr>
<td>8. Seek and act upon feedback.</td>
</tr>
<tr>
<td><strong>Undertake Safety Risk Assessment</strong></td>
</tr>
<tr>
<td>9. Establish risk management.</td>
</tr>
<tr>
<td>10. Use appropriate methodology for risk assessment.</td>
</tr>
<tr>
<td>11. Obtain broad stakeholder input to risk assessment.</td>
</tr>
</tbody>
</table>
### Requirements for Patient Safety in Relation to E-health Systems and Applications

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>Mitigate identified patient safety risks.</td>
</tr>
<tr>
<td>13.</td>
<td>Maintain risk register(s).</td>
</tr>
</tbody>
</table>

### Manage Patient Safety Across the E-health System Lifecycle

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>Use appropriate methodology to define the clinical problem(s) at hand and their patient safety dimensions.</td>
</tr>
<tr>
<td>16.</td>
<td>Engage clinicians.</td>
</tr>
<tr>
<td>17.</td>
<td>Define patient safety issues related to the clinical areas being addressed.</td>
</tr>
<tr>
<td>18.</td>
<td>Commence documenting the safety case.</td>
</tr>
<tr>
<td>19.</td>
<td>Ensure high quality processes for specification of requirements for safe e-health systems and applications and their enabling technologies.</td>
</tr>
<tr>
<td>20.</td>
<td>Analyse potential solutions.</td>
</tr>
<tr>
<td>22.</td>
<td>Take an architectural approach to patient safety.</td>
</tr>
<tr>
<td>23.</td>
<td>Undertake change management planning.</td>
</tr>
<tr>
<td>24.</td>
<td>Update the safety case.</td>
</tr>
<tr>
<td>26.</td>
<td>Assure patient safety in the procurement of e-health systems and applications.</td>
</tr>
<tr>
<td>27.</td>
<td>Test for patient safety.</td>
</tr>
<tr>
<td>28.</td>
<td>Ensure clinician engagement during implementation.</td>
</tr>
<tr>
<td>29.</td>
<td>Train and support in the use of e-health.</td>
</tr>
<tr>
<td>30.</td>
<td>Manage safety critical functions.</td>
</tr>
<tr>
<td>31.</td>
<td>Monitor clinical information systems.</td>
</tr>
</tbody>
</table>
### Requirements for Patient Safety in Relation to E-health Systems and Applications

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>Ensure patient safety is addressed in security controls.</td>
</tr>
<tr>
<td>33.</td>
<td>Ensure ongoing user training and support.</td>
</tr>
<tr>
<td>34.</td>
<td>Govern and maintain clinical knowledge.</td>
</tr>
<tr>
<td>35.</td>
<td>Manage authorisations.</td>
</tr>
<tr>
<td>36.</td>
<td>Articulate the responsibilities of system users.</td>
</tr>
<tr>
<td>37.</td>
<td>Assure clinical process continuity.</td>
</tr>
<tr>
<td>38.</td>
<td>Communicate concerning the status of system interfaces.</td>
</tr>
<tr>
<td>40.</td>
<td>Preserve patient safety information.</td>
</tr>
<tr>
<td>41.</td>
<td>Dispose securely in order to protect patient safety.</td>
</tr>
</tbody>
</table>

### Measure and Provide Feedback on Patient Safety

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.</td>
<td>Baseline patient safety metrics associated with e-health.</td>
</tr>
<tr>
<td>43.</td>
<td>Establish incident reporting that identifies where e-health may be implicated in patient safety incidents.</td>
</tr>
<tr>
<td>44.</td>
<td>Respond to patient safety incidents.</td>
</tr>
<tr>
<td>45.</td>
<td>Collaborate with other organisations that supply or receive clinical information or functionality to or from your organisation’s e-health systems and applications.</td>
</tr>
</tbody>
</table>
7. Incorporating Patient Safety into Enterprise Governance

This chapter presents the requirements of this Standard that are associated with incorporating patient safety into enterprise governance.

2. Document programs.
3. Appoint responsible officer(s).
5. Engage clinicians.
6. Promote cultures conducive to patient safety.
7. Communicate and consult with stakeholders.
8. Seek and act upon feedback.

The incorporation of patient safety into enterprise governance requires that:

- The highest-level decision makers (e.g. boards of directors, practice owners) are committed to promoting a culture of and mechanisms for safety in their organisations that explicitly incorporate patient safety in relation to e-health systems and applications.

- Health informaticians are diligent in undertaking their professional responsibilities to ensure that patient safety in their organisations is systematic and sustained.
**Requirement 1. Establish governance for patient safety in relation to e-health.**

**Organisations:**
Shall establish and maintain frameworks for managing patient safety in relation to e-health systems and applications that are fit for purpose and are integrated with other organisational frameworks.

Shall ensure that their framework for managing patient safety is tightly coupled with their frameworks for corporate and clinical governance, risk and quality management.

Should adopt the ethical practice statements defined in section 2 of this Standard.

Should provide resourcing to the levels required to assure the fitness for purpose of governance for patient safety in relation to e-health systems and applications.

**Health informaticians:**
Shall assure themselves that their organisation’s patient safety governance frameworks are fit for purpose.

Shall assure themselves about the quality of mechanisms to align patient safety in relation to e-health systems and applications with corporate and clinical governance, risk and quality management in their organisations.

**Requirement 2. Document programs.**

**Organisations:**
Shall document current initiatives addressing patient safety in relation to e-health systems and applications, in a form that enables:

- Identification of the patient safety portfolio, where more than one initiative exists;
- The allocation of priorities and responsibilities;
- The exercise of accountabilities;
- Communication and coordination;
- The assessment of outcomes against expectations; and
- Continuous improvement.

**Health informaticians:**
Shall assure themselves that their organisation’s programs are appropriately documented.
### Requirement 3.  
**Appoint responsible officer(s).**

<table>
<thead>
<tr>
<th><strong>Organisations:</strong></th>
<th><strong>Health informaticians:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall designate an officer with primary responsibility for clinical informatics in their organisation.</td>
<td>Shall ensure they are aware who has designated responsibilities for e-health systems and applications both in their own organisations and within organisations that can impact on their organisation’s patient safety.</td>
</tr>
<tr>
<td>Shall designate an officer with primary responsibility for patient safety in relation to e-health systems and applications.</td>
<td>Shall ensure they are aware who has designated responsibilities for patient safety in relation to e-health systems and applications both in their own organisations and within organisations that can impact on their organisation’s patient safety.</td>
</tr>
<tr>
<td>Shall provide responsible officers with authorities, training and resources commensurate with expectations of their roles.</td>
<td>Shall ensure that they are aware of appropriate escalation pathways within their organisations.</td>
</tr>
</tbody>
</table>

### Requirement 4.  
**Articulate responsibilities for patient safety in relation to e-health.**

<table>
<thead>
<tr>
<th><strong>Organisations:</strong></th>
<th><strong>Health informaticians with designated responsibilities for e-safety:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall promote the culture that patient safety is everybody’s business.</td>
<td>Shall ensure that the requirements associated with these responsibilities are clearly articulated, current and endorsed by their organisations.</td>
</tr>
<tr>
<td>Shall clearly articulate, endorse and maintain specific requirements for all staff members and agents with designated responsibilities per Requirement 3.</td>
<td></td>
</tr>
<tr>
<td>Organisations:</td>
<td>Health informaticians with designated responsibilities for e-safety:</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shall ensure these responsibilities are included in the staff development and performance assessment programs for staff members and agents with designated responsibilities.</td>
<td>Shall ensure that their competencies are commensurate with their e-safety responsibilities.</td>
</tr>
</tbody>
</table>

An example of a requirements statement is provided in Part C – Supporting Resources

### Requirement 5. Engage clinicians.

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall ensure that patient safety in relation to e-health systems and applications is explicitly included in organisational clinical governance.</td>
<td>Shall assure themselves that clinical engagement mechanisms in their organisations are fit for this purpose.</td>
</tr>
<tr>
<td>Shall ensure that practicing clinicians are involved in all levels of safety-related decision making that impact the use of clinical information systems.</td>
<td>Shall ensure they are competent in clinical engagement approaches and techniques.</td>
</tr>
</tbody>
</table>

### Requirement 6. Promote cultures conducive to patient safety.

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall promote patterns of behaviour that build commitment to and proficiency of management of patient safety within their spheres of control.</td>
<td>Shall lead by example, demonstrating values, exhibiting attitudes, developing and maintaining competencies, and modelling patterns of behaviour that are conducive to patient safety.</td>
</tr>
<tr>
<td>Should advocate for patterns of behaviour that build commitment to and proficiency of management of patient safety within their spheres of influence.</td>
<td>Should advocate for patterns of behaviour that build commitment to and proficiency of management of patient safety amongst other e-safety stakeholders.</td>
</tr>
</tbody>
</table>
### Requirement 7. Communicate and consult with stakeholders.

**Organisations:**
Shall develop and implement processes for effective communication and consultation concerning patient safety within their organisations.

Should communicate regarding patient safety in relation to e-health systems and applications with other organisations that can impact on their own organisation’s patient safety.

**Health informaticians:**
Shall assure themselves that communication and consultation concerning patient safety in relation to e-health systems and applications is effective in their organisation.

Should be pro-active in communicating and consulting regarding patient safety.

### Requirement 8. Seek and act upon feedback.

**Organisations:**
Shall ensure that:

- Metrics that are fit-for-purpose are developed, implemented and monitored.
- Reporting of patient safety hazards and incidents that are associated with e-health systems and applications is encouraged.
- Responses to such feedback are formulated and actioned on a timely basis.
- Where no response is deemed to be required, the reasons are clearly articulated, recorded and communicated to relevant stakeholders.

**Health informaticians:**
Shall assure themselves that fit-for-purpose metrics are developed, implemented and monitored.

Should be pro-active in ensuring that responses to feedback are formulated and actioned on a timely basis.
8. Undertake Patient Safety Risk Assessment

This chapter presents the requirements of this Standard that are associated with undertaking patient safety risk assessment.

9. Establish risk management.  
10. Use appropriate methodology for risk assessment.  
11. Obtain broad stakeholder input to risk assessment.  
12. Mitigate identified patient safety risks.  
13. Maintain risk register(s).  

Risk management is fundamental to patient safety, and effective risk assessment can be considered a critical success factor.


<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall specifically address patient safety in relation to e-health systems and applications in their risk management activities.</td>
<td>Shall assure themselves that risk management has been explicitly addressed within their organisations, and within organisations that can impact on their own organisation’s patient safety.</td>
</tr>
</tbody>
</table>
Requirement 10. Use appropriate methodology for risk assessment.

Organisations:
Shall use appropriate methodologies for assessing risks. For example, AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines is widely used in Australia as an overarching risk management framework.

Health Informaticians:
Shall assure themselves that their organisations’ risk management methodologies, risk appetites and risk tolerances:
- Are based on sustainable good practice.
- Cater for and are consistent with specific clinical information system initiatives.

Shall articulate their risk tolerances in relation to the implementation and use of e-health systems and applications, permitting assessment of whether or not a state of patient safety exists.

Requirement 11. Obtain broad stakeholder input to risk assessment.

Organisations:
Should consult and communicate broadly in establishing the contexts for assessing risks associated with e-health systems and applications.

Health Informaticians:
Shall assure themselves that risk assessments are sufficiently comprehensive, based on effective stakeholder engagement.

Requirement 12. Mitigate identified patient safety risks.

Organisations:
Should establish a risk mitigation plan for any identified risk assessed as being above the designated risk tolerance level.

Health Informaticians:
Should assure themselves that risk mitigations for e-health systems and applications are appropriate, based on effective stakeholder engagement.

Should allocate every identified risk to a risk owner, and ensure that each owner accepts ownership of their allocated risks.
### Requirement 13. Maintain risk register(s).

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall maintain a register of patient safety risks in relation to e-health systems and applications that accords with good practice in risk management.</td>
<td>Shall assure themselves that the risk register is appropriately managed.</td>
</tr>
</tbody>
</table>

A sample risk register is provided in Part C – Supporting Resources


<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should disclose the boundaries of risk controls pertaining to e-health systems and applications prior to any exchange of ownership or right of use to other stakeholders.</td>
<td>Shall advocate that supplier organisations disclose residual risks that may exist in e-health systems and applications prior to any exchange of ownership or right of use.</td>
</tr>
<tr>
<td>Should include in contracts pertaining to e-health systems and applications a requirement to discuss risk controls and outsourced risk.</td>
<td>In organisations acquiring e-health systems and applications should seek information on inherent risks, risk mitigations and residual risks, as part of due diligence activities.</td>
</tr>
<tr>
<td>Should explicitly plan for the mitigation of residual risks.</td>
<td></td>
</tr>
</tbody>
</table>
9. Manage Patient Safety Across the E-Health System Lifecycle

This chapter presents the requirements of this Standard that are associated with managing patient safety across the e-health system lifecycle.

15. Use appropriate methodology to define the clinical problem(s) at hand and their patient safety dimensions.
16. Engage clinicians.
17. Define patient safety issues related to the clinical areas being addressed.
18. Commence documenting the safety case.
19. Analyse potential solutions.
20. Ensure high quality processes for specification of requirements for safe e-health systems and applications.
22. Take an architectural approach to patient safety.
23. Undertake change management planning.
24. Update the safety case.
26. Assure patient safety in the procurement of e-health systems and applications.
27. Test for patient safety.
28. Ensure clinician engagement during implementation.
29. Train and support in the use of e-health systems and applications.
30. Manage safety critical functions.
31. Monitor e-health systems and applications.
32. Ensure patient safety is addressed in security controls.
33. Ensure ongoing user training and support.
34. Govern and maintain clinical knowledge.
35. Manage authorisations.
36. Articulate the responsibilities of system users.
37. Assure clinical process continuity.
38. Communicate concerning the status of system interfaces.
40. Preserve patient safety information.
41. Dispose securely in order to protect patient safety.
The requirements provided in this section address specific elements of system lifecycle management that are highlighted in patient safety literature as involving specific risks. This section is not intended to comprise a comprehensive guide to managing e-health systems and applications across their lifecycles.

Patient safety in relation to clinical information systems requires active management at all points in the system lifecycle, not just during implementation. In addition, because e-health systems and applications are developed for, implemented and operated in socio-technical contexts, the application of human factors methods are crucial throughout their life cycles.

The following six phase lifecycle for e-health systems and applications is synthesised from various sources and used to structure this section of the Standard. Some of the patient safety requirements associated with these phases are highlighted in the red boxes, for illustrative purposes.

**Figure 3 - E-Health System / Application Life Cycle Model**
The six phases of the lifecycle, depicted in Figure 3, are:

1. **Define the problem** – this incorporates assessing the feasibility of dealing with the clinical domain(s) being addressed, in various ways. This phase provides opportunities to: thoroughly assess current and potential patient safety hazards; articulate the most clinically appropriate ways of mitigating them; and articulate how new clinical information systems could best support this.

2. **Plan for a solution** – this incorporates conceptualisation, analysis, articulation of requirements and solution design. While the previous phase focused on analysis of the clinical issues being addressed, this phase focuses in more detail on how these clinical issues will be met by a clinical information system. It provides the opportunity: to plan for patient safety across the entire system lifecycle; ensure that all identifiable hazards are addressed; and articulate specific patient safety requirements and risk tolerances that can guide obtaining a new system.

3. **Obtain an e-health system** – this incorporates acquisition options analysis, procurement, acquisition / development / customisation and testing. This phase is critical in ensuring that the system to be acquired addresses patient safety satisfactorily across the entire clinical information system lifecycle.

4. **Implement the system** – this incorporates human, physical and other capacity building, piloting, migration planning, going live and post-implementation. This phase incorporates the opportunities to: enhance patient safety culture; provide system operators with the knowledge and skills they need to assure patient safety; assure that the system and associated workflows operate as envisaged; and ensure important patient safety hazards are addressed before the system is widely deployed.

5. **Operate and maintain the system** – this incorporates ongoing usage, routine upkeep, review, evaluation and revision. This phase typically represents 80% of the system lifecycle and accordingly is the most critical phase for clinical governance assuring that patient safety is managed. This includes: managing the quality and application of clinical data, information and knowledge addressed by and embedded in the e-health(s); ensuring clinical process continuity; and ensuring continuous improvements in patient safety.

6. **Dispose of the system** – this incorporates planning for decommissioning, archival and disposal. This phase incorporates the responsibility to ensure that learnings from the system and its usage are captured in order to inform future initiatives; and to preserve and dispose of clinical data, information and knowledge securely.
9.1 Define the Problem

Effectively defining the problem(s) that an e-health system / application is intended to resolve or assist with is the fundamental basis for clinical IT. By definition, ensuring that a system is fit for purpose – including meeting patient safety requirements - means that the purpose(s) must be clearly articulated and that there is shared understanding of that articulation. There may be scenarios in which patient safety is optimised not by using (new) clinical information systems, but by redesigning a clinical practice or workflow.

Requirement 15. Use appropriate methodology to define the clinical problem(s) at hand and their patient safety dimensions.

Organisations:

Shall use appropriate problem-solving methodologies for articulating the problem(s) that e-health is proposed to resolve or assist.

Should ensure that staff and agents engaged in problem definition are competent in such activities.

Health Informaticians:

Should undertake due diligence to ensure that problem definitions concerning clinical IT are of high quality.

Shall maintain competence in problem definition.

Requirement 16. Engage clinicians.

Organisations:

Shall ensure that local clinicians are engaged from the outset in all phases of the system lifecycle.

Should ensure that clinicians in leadership positions are supported to be directly involved in the implementation and ongoing review of e-health systems and applications.

Health Informaticians:

Shall maintain awareness of good practices in clinical engagement and socio-technical environments.

Shall assure themselves that clinical engagement strategies used in their organisations are effective and sufficient.

Shall take appropriate action to address situations where inadequate clinical engagement is evident.
**Organisations:**

Should ensure that e-health initiatives:

- Are coherent with the values and ethos of the clinical workforce and the organisation.
- Feature ongoing, open dialogue with clinicians that builds relationships and engenders mutual trust and respect.
- Cater for the time and effort required for clinical engagement.

**Health Informaticians:**

- Define patient safety issues related to the clinical areas being addressed.

**Organisations:**

- Shall ensure that existing and potential patient safety issues are identified during articulation of the contexts associated with the problem(s) at hand.
- Shall ensure that problem definition statements are validated, agreed and where necessary prioritised by the key stakeholders concerned.

**Health Informaticians:**

- Shall assure themselves that there is clear and shared understanding of the problem(s) that the e-health system is proposed to resolve or assist, including that priorities are agreed as required.

**Requirement 18.** Commence documenting the safety case.

**Organisations:**

- Should initiate a safety case for proposed e-health system solutions at the earliest opportunity – problem definition.

**Health Informaticians:**

- Should advocate for documentation of a safety case from the earliest possible opportunities.
The safety case comprises documentation that confirms that the development, deployment and use of e-health systems and applications will not pose an unacceptable level of safety risk. Safety cases are widely used in safety critical industries / scenarios.

The e-safety case is established and maintained over the system life cycle.

**Requirement 19. Analyse potential solutions.**

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall ensure that the feasibilities of multiple solutions are assessed, including those not associated with e-health systems and applications.</td>
<td>Shall assure themselves that proposed e-health solutions have been selected using a professional approach.</td>
</tr>
<tr>
<td>Shall ensure that patient safety is explicitly included in the criteria used to assess potential solutions.</td>
<td></td>
</tr>
</tbody>
</table>
9.2 Planning for Solution(s)

From a safety perspective, three key elements of the planning phase warrant particular attention – analysing requirements, architecting solutions and planning the system’s lifecycle.

Requirement 20. Ensure high quality processes for specification of requirements for safe e-health systems and applications.

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall use system planning methodologies that take into account the “information paradox” – which is that stakeholders often show insufficient understanding of requirements and their implications in the early stages of a project, where requirement specification processes may be concentrated.</td>
<td>Should maintain knowledge of methodologies for the specification of requirements.</td>
</tr>
<tr>
<td>Shall ensure that competent resources are used to articulate requirements and their implications for e-health systems and applications.</td>
<td>Should maintain competence in requirement specification sufficient to provide due diligence to such processes.</td>
</tr>
<tr>
<td>Should use industry standard methodologies for the specification of patient safety requirements.</td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall explicitly articulate patient safety requirements for e-health systems and applications.</td>
<td>Shall assure themselves that patient safety has been taken into account during the specification of requirements for e-health systems and applications.</td>
</tr>
<tr>
<td>Shall ensure that all hazards identified during the definition stage are considered during requirement specification processes.</td>
<td></td>
</tr>
<tr>
<td>Organisations:</td>
<td>Health Informaticians:</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Should endorse these patient safety requirements as being aligned with the</td>
<td>Shall maintain awareness of standards and</td>
</tr>
<tr>
<td>organisation’s overall risk appetite and the risk tolerance associated with</td>
<td>specifications that describe requirements</td>
</tr>
<tr>
<td>the specific initiative.</td>
<td>for clinical IT that are associated with</td>
</tr>
<tr>
<td>Should include requirement specifications in the following safety-critical</td>
<td>safety and quality.</td>
</tr>
<tr>
<td>areas at a minimum:</td>
<td></td>
</tr>
<tr>
<td>- Human-computer interfaces that are designed according to human factors</td>
<td></td>
</tr>
<tr>
<td>principles and ensure that required information is visible, readable, and</td>
<td></td>
</tr>
<tr>
<td>understandable.</td>
<td></td>
</tr>
<tr>
<td>- Processes and procedures that ensure accurate patient identification at</td>
<td></td>
</tr>
<tr>
<td>each step in the clinical workflow.</td>
<td></td>
</tr>
<tr>
<td>- Role-based access to ensure that all applications, features, functions,</td>
<td></td>
</tr>
<tr>
<td>and patient data are accessible only to users with appropriate levels of</td>
<td></td>
</tr>
<tr>
<td>authorisation.</td>
<td></td>
</tr>
<tr>
<td>- Protocols for exchanging data with other systems, both inside and outside</td>
<td></td>
</tr>
<tr>
<td>the organisation’s boundaries.</td>
<td></td>
</tr>
<tr>
<td>- Use of clinically appropriate terms.</td>
<td></td>
</tr>
<tr>
<td>- Use of recommended international, national and jurisdictional standards</td>
<td></td>
</tr>
<tr>
<td>for clinical data.</td>
<td></td>
</tr>
<tr>
<td>Where clinical decision support features and functions are involved,</td>
<td></td>
</tr>
<tr>
<td>organisations should:</td>
<td></td>
</tr>
<tr>
<td>- Adopt national recommendations on the principles and desirable features of</td>
<td></td>
</tr>
<tr>
<td>clinical decision support systems.</td>
<td></td>
</tr>
<tr>
<td><strong>Organisations:</strong></td>
<td><strong>Health Informaticians:</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>• Develop or modify clinical content based on evidence, relying, where available, on nationally recognised, consensus-based recommendations.</td>
<td></td>
</tr>
<tr>
<td>• Ensure that clinicians are able to override computer-generated clinical interventions when they deem it necessary.</td>
<td></td>
</tr>
</tbody>
</table>

**Requirement 22.** Take an architectural approach to patient safety.

<table>
<thead>
<tr>
<th><strong>Organisations:</strong></th>
<th><strong>Health Informaticians:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall consider patient safety in the context of the overall system, not individual components such as the software.</td>
<td>Shall maintain understanding of:</td>
</tr>
<tr>
<td>Shall consider human factors and user-centred design throughout</td>
<td>• The importance of architecture to safety.</td>
</tr>
<tr>
<td></td>
<td>• Enterprise architecture concepts sufficient to identify that an architectural approach to patient safety is in place.</td>
</tr>
<tr>
<td></td>
<td>• Human factors and user-centred design</td>
</tr>
<tr>
<td>Shall ensure that all hazards identified during the definition stage are mitigated, if possible, in the overall system architecture.</td>
<td></td>
</tr>
<tr>
<td>Should ensure that architectural patterns associated with safety critical systems (e.g. fail-safe behaviours, redundancy) are considered.</td>
<td></td>
</tr>
</tbody>
</table>
Requirement 23. **Undertake change management planning.**

**Organisations:**
Shall explicitly assess change management requirements and capabilities associated with ensuring patient safety, realistically assessing gaps and how they will be filled.

**Health Informaticians:**
Shall maintain competence in explaining methods for change management.  
(Note: this is one of the 52 competencies required of health informaticians under the [Australian] Health Informatics Competencies Framework (HISA, 2013)).

Shall advocate for change management approaches that are likely to be effective in the relevant context.

Requirement 24. **Update the safety case.**

**Organisations:**
Should update the safety case to describe considerations and decisions taken during planning.

**Health Informaticians:**
Should advocate for comprehensive documentation of patient safety at all stages of the system lifecycle.

### 9.3 Obtaining Solution(s)

Maintaining focus and momentum on patient safety through the processes of obtaining e-health systems and applications, whether through procurement (adoption), development or elements of both (adaption), is crucial. Tradeoffs are often made, or made explicit, during these processes.

Where an e-health product or service is procured from the market, the requirements described in this section are applied via the procurement processes. Where the product or service is developed, they are applied via project management processes. For clarity, this means that:

- From the perspective of an acquirer (e.g. a health service):
  - Where an e-health product or service is purchased “off-the shelf” (i.e. adopted), the requirements described in this section are applied via procurement processes.
  - Where an e-health product or service is purchased subject to modifications undertaken by the supplier(s) (i.e. adapted), the requirements described in this section are applied via procurement processes.
Where the bespoke development of an e-health product or service is purchased, the requirements described in this section are applied via procurement processes.

Where the bespoke development of an e-health product or service is undertaken in-house, the requirements described in this section are applied via project management processes.

- From the perspective of a supplier of an e-health product or service (e.g. a software developer/vendor), the requirements described in this section are applied via project management processes.

- Where the acquisition models are mixed (e.g. joint development or customisation via collaboration between supplier(s) and acquirer(s), the requirements described in this section are applied via both procurement and project management processes.

**Requirement 25.**  **Undertake patient safety assessment of the development of e-health systems and applications.**

**Organisations:**

Shall establish, document and maintain, throughout the system life cycle, an ongoing patient safety process that identifies clinical hazards, estimates and evaluates associated clinical risks, mitigates these risks, and monitors the effectiveness of the mitigations throughout the life cycle.

Shall compile a date-stamped pre-release safety case report.

**Health Informaticians:**

Shall assure themselves that processes for managing patient safety during the development of e-health systems and applications are appropriate and sufficient.

Shall apply due diligence to safety cases and, where appropriate, advocate for enhancement of their quality.
<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall, prior to release for distribution or deployment of the e-health system / application, undertake and document rigorous review of the application of the patient safety assurance process. This review shall at least ensure that:</td>
<td></td>
</tr>
<tr>
<td>• The clinical risk management plan has been appropriately implemented and its outcomes captured.</td>
<td></td>
</tr>
<tr>
<td>• Overall residual clinical risk is acceptable using the criteria defined in the clinical risk management plan.</td>
<td></td>
</tr>
<tr>
<td>• Appropriate methods are in place to obtain relevant post-deployment information.</td>
<td></td>
</tr>
<tr>
<td>• A sufficient and accurate safety case has been produced.</td>
<td></td>
</tr>
<tr>
<td>Shall undertake, whenever the system is modified, clinical risk analysis commensurate with the likelihood that new clinical risks may have been introduced.</td>
<td></td>
</tr>
<tr>
<td>Shall maintain an audit trail of all versions and patches released so as to provide traceability in the event of a hazard alert.</td>
<td></td>
</tr>
</tbody>
</table>

**Requirement 26.** Assure patient safety in the procurement of e-health systems and applications.

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall ensure that their patient safety requirements are effectively communicated to (potential) suppliers, and that the interpretation of these requirements by (potential) suppliers is accurate and sufficient.</td>
<td>Shall maintain competency in the articulation of requirements. (Note: this is one of the 52 competencies required of health informaticians under the [Australian] Health Informatics Competencies Framework (HISA, 2013)).</td>
</tr>
<tr>
<td>Organisations:</td>
<td>Health Informaticians:</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Should request and take into consideration developers’ safety case reports and the appropriateness of intended use of the system.</td>
<td>Should maintain awareness of contractual issues with the potential to compromise patient safety.</td>
</tr>
<tr>
<td>Should establish agreements or contract terms with business partners and vendors that address the management of safety risks, including the sharing of risks or risk transfer (outsourcing) as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Should explicitly identify aspects of “hold harmless” and related clauses that have the potential to compromise patient safety and negotiate for their mitigation, including via the articulation of the scope of “learned intermediaries”.</td>
<td></td>
</tr>
</tbody>
</table>

**Requirement 27. Test for patient safety.**

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall articulate and agree, between all relevant stakeholders, comprehensive testing plans for e-health systems and applications that should normally include: unit testing; integration testing; functional testing; system testing; usability testing; and acceptance testing. The testing regime shall address and trace back to requirements associated with patient safety.</td>
<td>Shall maintain competency in testing concepts and methodologies.</td>
</tr>
<tr>
<td>Should incorporate testing under normal, abnormal and emergency conditions.</td>
<td>Shall assure themselves that testing for e-health systems and applications has been sufficient to reasonably identify patient safety issues.</td>
</tr>
</tbody>
</table>
9.4 Implementation

Implementations always involve change to the way things happen. Change is the way that either benefits are realised or, as unfortunately happens from time to time, harm is done.


**Organisations:**

Should ensure that implementations in clinical settings are treated as socio-technical change processes, including by:

- Exploring and exploiting the flexibility of systems for local customisation.
- Assessing customisation in the light of local circumstances.
- Upskilling clinicians with regard to patient safety.
- Ensuring clinicians can consistently get timely and non-interruptive access to infrastructure such as workstations.
- Ensuring health informatics skills are available to support clinicians.

**Health Informaticians:**

Should satisfy themselves that clinician engagement is sufficiently wide and deep during the implementation phase.

Should take appropriate action to address situations where clinical engagement is not adequate.

---

Requirement 29. Train and support in the use of e-health systems and applications.

**Organisations:**

Shall ensure that training and support are readily available, tailored to and are sufficient for the needs of e-health system and application users.

**Health Informaticians:**

Shall assure themselves that training and support are:

- Based upon sound analysis of clinical training needs and good practice in the delivery of training and support.
- Appropriately tailored for context; readily available to users; and sufficient for their needs.
<table>
<thead>
<tr>
<th>Requirement 30.</th>
<th>Manage safety critical functions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisations:</strong></td>
<td>Shall ensure that safety critical functions associated with and/or supported by e-health systems and applications are clearly identified, managed and reviewed on a regular basis.</td>
</tr>
<tr>
<td><strong>Health Informaticians:</strong></td>
<td>Shall undertake due diligence to ensure that safety critical functions associated with and/or supported by clinical IT are identified, managed and reviewed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement 31.</th>
<th>Monitor e-health systems and applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisations:</strong></td>
<td>Should closely monitor e-health systems and applications after go-live, with a view to prevention and early identification of patient safety issues. Shall ensure that rapid response mechanisms for patient safety issues are available as required.</td>
</tr>
<tr>
<td><strong>Health Informaticians:</strong></td>
<td>Shall assure themselves that patient safety issue detection systems are in place and regularly reviewed.</td>
</tr>
</tbody>
</table>
Requirement 32. Ensure patient safety is addressed in security controls.

**Organisations:**

Shall ensure that e-health assets are protected and their quality assured.

**Health Informaticians:**

Shall maintain competency in the protection of information assets.

9.5 Operation and Maintenance of E-Health Systems and Applications

The transition between the implementation and operation and maintenance stages of the systems life cycle is often accompanied by a series of other transitions, such as from:

- Project (discrete, devoted) funding to funding from a recurrent pool of funds.
- Project management to more generic business and clinical governance mechanisms.
- High visibility of the system to “day-to-day” modes of operation, particularly in areas such as change management, training and support.

Just as clinical handovers are known to be areas though which safety issues often arise, so are organisational handovers such as the above.

Requirement 33. Ensure ongoing user training and support.

**Organisations:**

Shall ensure that:

- New staff and agents who are expected to use e-health systems and applications are appropriately trained in and have access to information and support regarding patient safety issues.
- Experienced users are appropriately trained in and have access to information and support about system changes.
- The currency and quality of training and support resources are maintained, including incorporating

**Health Informaticians:**

Shall assure themselves that ongoing training and support are effective and sufficient.
feedback from system users.

Should ensure that appropriate information and/or other support is available to patients/consumers who use clinical information systems:

- That they expose to patients/consumers (e.g. patient access to health records via patient portals; health apps provided by/through the health service provider).
- Via which they provide clinical information (e.g. consumer health knowledgebases).

<table>
<thead>
<tr>
<th>Should take appropriate action in situations where ongoing user training and support is inadequate.</th>
</tr>
</thead>
</table>

**Requirement 34. Govern and maintain clinical knowledge.**

**Organisations:**

Shall ensure that clinical knowledge, rules, and logic embedded in clinical information systems are reviewed and addressed regularly, as well as whenever changes are made in related systems.

Shall ensure that all such reviews and changes are endorsed by clinical governance.

**Health Informaticians:**

Shall identify where clinical knowledge, rules, and logic are embedded in clinical information systems.

Shall assure themselves that there is clinical governance of such clinical knowledge, rules, and logic.

**Requirement 35. Manage authorisations.**

**Organisations:**

Shall implement controls to assure that e-health systems and applications are used as authorised; safety critical procedures are adhered to; and legal and regulatory requirements are met.

**Health Informaticians:**

Are aware of and enable authorisation and regulation.
### Requirement 36. Articulate the responsibilities of system users.

**Organisations:**
- Shall articulate the responsibilities of system users with respect to patient safety.
- Shall ensure these responsibilities are communicated to system users.
- Shall implement measures to encourage uptake of these responsibilities.

**Health Informaticians:**
- Shall maintain awareness of the responsibilities of system users with respect to patient safety.
- Shall demonstrate leadership in uptake of these responsibilities.
- Should encourage other system users to take up these responsibilities.

### Requirement 37. Assure clinical process continuity.

**Organisations:**
- Shall ensure that patient safety is specifically addressed via business continuity capabilities.
- Shall ensure that processes are in place to ensure clinical data integrity during and after major system changes.
- Shall ensure that:
  - Downtime and reactivation policies and procedures are complete, available, and reviewed regularly.
  - Staff are trained and tested on downtime and recovery procedures.
  - A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.
- Shall ensure that ongoing hazard identification and mitigation is undertaken.

**Health Informaticians:**
- Shall assure themselves that clinical business continuity measures are in place to ensure patient safety.
- Shall maintain awareness of contemporary business continuity issues and approaches.
**Requirement 38.** Communicate concerning the status of system interfaces.

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall ensure that people involved in maintenance or use of system interfaces are notified when changes are made that affect the content of the standard data files or allowable values transmitted via the interface(s).</td>
<td>Shall maintain awareness of the interfaces enabling or enabled by e-health systems and applications, and the associated patient safety risks.</td>
</tr>
<tr>
<td>Shall ensure that the operational status of system interfaces is clear to users with regard to clinical use, (e.g. knowing when the interface cannot transmit or receive messages, alerts or crucial information).</td>
<td></td>
</tr>
</tbody>
</table>
9.6 Decommissioning and Disposal

The decommissioning and disposal of e-health systems and applications has the potential to involve clinical risk, for example where functionality is removed from clinical settings that is relied upon by clinicians; where the removal of functionality is not well planned for or communicated to clinicians; or where disruption to clinical practice results.


Organisations:
Should evaluate patient safety associated with the system before decommissioning it, including undertaking consequence analysis in respect of removal of the system.

Health Informaticians:
Should maintain competency in consequence analysis.


Organisations:
Shall ensure that key information about e-health systems and applications that is pertinent to patient safety is preserved in the event that these systems are reactivated in the future.

Health Informaticians:
Shall ensure that key information from e-health systems and applications that is pertinent to patient safety is preserved so that it can continue to be used.

Requirement 41. Dispose securely in order to protect patient safety.

Organisations:
Shall ensure that measures are in place to prevent inadvertent loss or exposure of sensitive data when clinical information is disposed of.

Health Informaticians:
Should assure themselves that measures are in place to prevent the loss or exposure of sensitive data when clinical information is disposed of.
10. **Measure and Provide Feedback on Patient Safety**

This chapter presents the requirements of this Standard that are associated with measuring and providing feedback on patient safety.

42. Baseline patient safety metrics associated with e-health systems and applications.
43. Establish incident reporting that identifies where e-health systems and applications may be implicated in patient safety incidents.
44. Respond to patient safety incidents.
45. Collaborate with other organisations that supply or receive clinical information or functionality to or from your organisation’s e-health systems and applications.

Measurement, monitoring and feedback on patient safety is crucial to: maintaining a safe clinical environment, enhancing safety culture, and improving the safety and quality of e-health.

**Requirement 42.** Baseline patient safety metrics associated with e-health systems and applications.

<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should identify, measure and monitor risk tolerance/ acceptability levels associated with clinical practices that are expected to be impacted by e-health initiatives.</td>
<td>Should maintain competence in the measurement of risk tolerances and their application.</td>
</tr>
</tbody>
</table>
**Requirement 43.** Establish incident reporting that identifies where e-health systems and applications may be implicated in patient safety incidents.

<table>
<thead>
<tr>
<th><strong>Organisations:</strong></th>
<th><strong>Health Informaticians:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Shall encourage the reporting and other identification of harmful incidents, near misses and hazards that users and other stakeholders recognise or suspect may be associated with e-health systems and applications.</td>
<td>Shall maintain competency in the development, implementation and use of clinical and IT incident reporting systems.</td>
</tr>
<tr>
<td>Shall train clinical information supporting resources (e.g. help desk staff) to identify and report on potential patient safety issues.</td>
<td></td>
</tr>
<tr>
<td>Shall ensure that all reporting systems that may be used to capture patient safety incidents (including IT help desks) are configured to report consistently and that patient safety reports are harvested from all such systems.</td>
<td></td>
</tr>
<tr>
<td>Should incorporate the following elements into incident reporting systems:</td>
<td></td>
</tr>
<tr>
<td>- Blame free reporting and the capability for anonymous reporting as appropriate.</td>
<td></td>
</tr>
<tr>
<td>- Simplified and accessible reporting.</td>
<td></td>
</tr>
<tr>
<td>- Identification of incidents in which clinical information systems may be implicated (allowing further analysis).</td>
<td></td>
</tr>
<tr>
<td>- Education and training that provides clarity on what should be reported; how the reporting system works; and how report leads to improvements in patient safety and clinical satisfaction.</td>
<td></td>
</tr>
<tr>
<td>- Timely feedback.</td>
<td></td>
</tr>
<tr>
<td>Should, where feasible, integrate this reporting with other patient safety reporting.</td>
<td></td>
</tr>
</tbody>
</table>
### Requirement 44. Respond to patient safety incidents.

**Organisations:**
- Should maintain the capacity to respond to reported patient safety incidents on a timely basis.
- Should take immediate steps to manage harmful incidents or near-misses and to mitigate risks.
- Should document procedures for managing patient safety incidents associated with e-health systems and applications, including escalation protocols and contingency plans.
- Should maintain clinical audit trails, enabling analysis and investigation.
- Shall provide feedback on e-safety issues and responses to their clinical and information governance functions.
- Should provide appropriate feedback on e-safety issues and responses to the wider e-safety community.

**Health Informaticians:**
- Should maintain awareness of their organisation’s patient safety incident reporting systems.

### Requirement 45. Collaborate with other organisations that supply or receive clinical information or functionality to or from your organisation’s e-health systems and applications.

**Organisations:**
- Should establish relationships and agreements with other organisations that either supply or receive their clinical information or functionality, to facilitate rapid resolution of patient safety incidents that may have implications for these other organisations.

**Health Informaticians:**
- Should assure themselves that adequate collaborative arrangements are in place with organisations that supply or receive clinical information or functionality.
<table>
<thead>
<tr>
<th>Organisations:</th>
<th>Health Informaticians:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where a flaw in an e-health product or service proves to be the cause of or a contributing factor to a patient safety incident, the organisation should immediately notify the distributor of the product or service.</td>
<td>Health Informaticians:</td>
</tr>
<tr>
<td>Where a flaw is confirmed in an e-health product or service, the distributor should notify all other customers of the product or service, who may be at risk of a similar incident.</td>
<td></td>
</tr>
</tbody>
</table>
11. Documentation

In summary, the specific documentation required by this standard comprises of the following.

11.1 Safety Program Documentation

Organisations involved with clinical information systems, whether as a designer/developer, supplier, implementer, operator, or user, need to document their overall programs for managing patient safety. Patient safety risks and issues may accumulate over a range of individual initiatives, so an overall picture is important. A program level approach also aims to ensure consistency of principles, optimisation of resources and effective prioritisation.

More information is available in Part C, Supporting Resources, but in summary patient safety program documentation comprises articulation of the organisation’s:

- E-health portfolio – what is the organisation’s involvement in clinical systems? What projects and ongoing operations is it involved with?
- Patient safety framework – who does what, how, why, when and where to assure safety? How is the framework itself maintained?
- Risk appetite – what is the broad-based amount of risk the organisation is willing to accept in pursuit of its mission or vision? Defined risk appetite provides the foundation for determining the risk tolerances for individual clinical information system initiatives.
- Risk assessment – the controls, mitigations in place, and risk acceptance

Safety program documentation may be standalone or it may be integrated into other program level / corporate documentation with which it needs to be aligned (e.g. IT and/or clinical governance). However, it must be discernable – i.e. specifically referenced as patient safety associated with an e-health system or application.
11.2 Risk Register(s)

Specific patient safety risks need to be identified, expounded, recorded and managed over the system lifecycle. The risk register is a primary control mechanism for managing these risks.

The risk register (risk log) should be a controlled document with an assigned responsible officer. Its purposes include:

- Enabling those involved to be kept aware of issues
- Providing a means of tracking response to issues as well as overall risk management performance.

This risk register may be incorporated into other risk registries as appropriate for the organisation. However, again, patient safety risks associated with a clinical information system must be discernable.

More information is available in Part C, Supporting Resources.

11.3 Safety Case

“Safety cases” are widely used in safety critical industries and scenarios. Safety cases are documents that confirm that the development, deployment and use of clinical information systems will not pose an unacceptable level of patient safety risk.

Safety cases need to be developed and maintained for all clinical information system initiatives. Their development should begin at the earliest opportunity, ideally in the problem definition phase, in order to ensure that the risk tolerance for the initiative is agreed and understood from the beginning, and that patient safety is explicitly included in design and/or the criteria used to assess potential solutions.

More information is available in Part C, Supporting Resources, but in summary safety cases should include:

- Description of the e-health initiative and the problem(s) it is proposed to resolve.
- Description of the associated patient safety context and risks.
- Evidence which is used as the basis of the patient safety argument(s), and supporting assumptions.
  Summaries of patient safety experiences for the initiative, built up over time and demonstrating achievement of or progress towards patient safety.
- Important learnings which will inform future patient safety management.
References


Office of the National Coordinator for Health Information Technology. 2014. Safety Assurance Factors for EHR Resilience (SAFER), System Configuration. U.S.A.

Office of the National Coordinator for Health Information Technology. 2014. Safety Assurance Factors for EHR Resilience (SAFER), System Interfaces. U.S.A.


# Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.01</td>
<td>13-03-2015</td>
<td>Initial draft for discussion</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.02</td>
<td>08-04-2015</td>
<td>Revisions after review by J Zelcer</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.03</td>
<td>12-06-2015</td>
<td>Revisions after review by T Williams</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.04</td>
<td>15-06-2015</td>
<td>Revision after resolution of outstanding queries from J Zelcer &amp; T Williams</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.05</td>
<td>18-08-2015</td>
<td>Revision following review by a panel of experts</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.06</td>
<td>09-09-2015</td>
<td>Revision after review by T Williams &amp; N Chartres</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.07</td>
<td>26-09-2015</td>
<td>Revision following feedback from Expert Group members</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.08</td>
<td>27/10/2015</td>
<td>Further revision following feedback from Expert Group members</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.09</td>
<td>25/01/2016</td>
<td>Further revision following feedback from experts at ISO</td>
<td>D Rowlands</td>
</tr>
<tr>
<td>V0.10</td>
<td>23/02/2016</td>
<td>Formatting and minor editing updates</td>
<td>L Schaper</td>
</tr>
</tbody>
</table>
The Digital Health Workforce Publication series is proudly brought to you by the Health Informatics Society of Australia

www.hisa.org.au