**DSC Notice: 14/2009 V1.2**
**Date of Issue: August 2010**

Information Standards Board for Health and Social Care

| Sponsoring Organisation: | Implementation Date: | 30 December 2009 |
|---|---|---|
| NHS Connecting for Health | Subject: Application of Patient Safety Risk Management to the Manufacture of Health Software | |

## DATA SET CHANGE NOTICE

This DSCN informs users of the approval of a new information standard by the Information Standards Board for Health and Social Care (ISB).

This was approved by ISB at its meeting on 29 April 2009.

**Summary:**
This standard specifies the risk management processes required to minimise risks to patient safety in respect to the manufacture of health software products either as new systems or as changes to existing systems.

The application of this standard will enable the manufacturers of health software to properly manage and mitigate clinical risks associated with the production of software and systems. It will not in itself guarantee a safe system, rather create the necessary environment and controls through which manufacturers and users can document and agree the levels of risk which are tolerable in specific application fields, and those which are not. In the case of those risks which are not tolerable, the standard gives a framework for designing, agreeing and evidencing the mitigation of the risk.

This notice is relevant to manufacturers of health software for the NHS as well as to those responsible for health software assurance and clinical safety assurance. Trusts and others purchasing systems for use in the NHS can use the standard immediately to support the procurement / contract process and must do so by 30 December 2009.

The standard sets out clinical safety management requirements for suppliers to the National Programme for IT and, as a pre-requisite, for all systems requesting connection to the National Care Records Spine service.

Other suppliers of health software to the NHS are expected to achieve conformance by 30 December 2009.

**Datasets / return affected:** None

**Related DSCNs:** DSCN 18/2009 (*Application of Patient Safety Risk Management to the Deployment and Use of Health Software*)

**Impact of Change:**

| | | | |
|---|---|---|---|
| **Service:** | Minor | **System Suppliers:** | Minor / Major depending on current practices |

The Information Standards Board for Health and Social Care (ISB) is responsible for approving information standards.

# DATA SET CHANGE NOTICE

| | |
|---|---|
| **Reference No:** | **DSCN 14/2009** |
| **Version No:** | **1.2** |
| **Type of Change:** | Introduction of a new approved Information Standard |
| **Implementation Date:** | **30 December 2009** |
| **Business Justification:** | This standard will address the lack of standards governing clinical safety management for health IT systems. The guidance and controls in the standard will allow for enhanced control of safety risks arising from poorly developed IT systems, and will contribute to increasing the likelihood that systems deployments will be successful. |
| **Effect on other Information Standards:** | Risk management at the interface between the manufacturer and the deploying organisation is also addressed in the related standard - Application of patient safety risk management to the deployment and use of health software (DSCN 18/2009). |

## Introduction

The application of this standard will enable the user to properly manage and mitigate clinical risks associated with the production of software and systems. It will not in itself guarantee a safe system, rather create the necessary environment and controls through which the users and manufacturers can document and agree the levels of risk which are tolerable in specific application fields, and the converse – those which are not. In the case of those risks which are not tolerable, this standard gives a framework for designing, agreeing and evidencing the mitigation of the risk.

The standard is specifically designed to address the increasingly common instance of computer systems errors-in-use and/or defects resulting in patients being at an increased risk of harm.

## Background

Information and communication technologies, including decision support, can bring substantial benefit to patients. However, unless they are safe and fit for purpose they may also present potential for harm. The potential for harm may arise from use of the systems or it may equally lie in the system design such as:

- Poor evidence base for design;
- Failure in design logic to properly represent design intentions;
- Failure in logic to represent good practice or evidence in the design phase;
- Poor or confusing presentation of information or poor search facilities;
- Failure to update in line with current knowledge.

The developers of this standard are working with a joint working group of international standards organisations undertaking a review of international medical devices standards. It is expected the group will consider including the scope of the NHS standard in its review. Implications for the NHS of any international developments will be considered as part of the scheduled reviews of this NHS standard by the NHS CFH Clinical Safety Group.

Software manufacturers deploying standard industry software safety engineering practices should experience little additional burden as a result of compliance to this standard, as a robust quality management system will produce the majority of the products required, as a by-product. There will

however be a significant impact on suppliers who have neglected to treat clinical systems with an appropriate rigour as would be demanded in other safety industries.

## Details of the Standard

The life cycle of a health software product includes design, production, deployment, use, maintenance and decommissioning. A manufacturer will be involved in design and production and may be involved in deployment particularly for complex systems. Where a customer contracts out responsibility for IT services to the manufacturer, the latter may also be involved in use of the application and decommissioning. This standard applies to all the life cycle phases in which the manufacturer is involved where this will depend on the contractual scope with the customer.

It applies to any health software product and connectivity to the product whether or not it is placed on the market and whether or not it is for sale or free of charge. Connectivity includes but is not limited to: message handler, message, message wrapper, security devices/card readers/cards & software, printer routines. The standard is intended to cover health software products which are not, in practice, covered by medical device regulations.

The standard provides manufacturers with guidance on appropriate controls to clinically verify/prove/validate any logic structures within software packages and is couched within the framework of controls established as part of the standard.

It forms the basis of a requirement placed on all suppliers at contract stage and the basis of assurance work performed by Trusts and NHS CFH in order to assess the fitness for purpose of systems delivered by suppliers. To this extent, it should be regarded as a compliance scheme.

To be compliant with the standard, the manufacturer must establish, document and maintain throughout the lifecycle an ongoing process for identifying clinical hazards associated with the health software product, estimating and evaluating the associated clinical risks, controlling these risks, and monitoring the effectiveness of the controls throughout the lifecycle. This process must include the following elements:

- context, requirements and scope identification;
- creation of clinical risk management plan;
- setting the requirements for and defining the competencies of personnel;
- clinical hazard identification;
- clinical risk analysis;
- clinical risk evaluation;
- clinical risk control;
- residual clinical risk acceptance;
- creation of clinical safety case report(s);
- post deployment monitoring;
- post-production maintenance of clinical risk management process.

Clinical assurance staff should use the standard as a benchmark in assessing whether or not a software system has undergone sufficiently rigorous hazard assessment and mitigation prior to deployment for management of patients.

***Timescales for Implementation***

| FRAMEWORK | Health and Social Care Personnel | Organisation[1] | IT Suppliers[2] |
|---|---|---|---|
| **Effective Date**[3] "may use" | Immediate | Immediate | Immediate |
| **Implementation Date**[4] "must use" | Not applicable | 30 December 2009 | 30 December 2009 |
| **Conformance Date**[5] "must be used effectively and assessed for use" | Not applicable | 30 December 2009 | 30 December 2009 |
| **Superseded Date (of prior standard)**[6] "stop using prior standard" | Not applicable | Not applicable | Not applicable |

## Effects on Other Information Standards

Risk management at the interface between the manufacturer and the deploying organisation is also addressed in the related standard - *Application of Patient Safety Risk Management to the Deployment and Use of Health Software* (DSCN 18/2009).

## Sponsor Details

Dr Charles Gutteridge
National Clinical Director for Informatics
NHS Connecting for Health

## Further Information and Support

Copies of the standard and details of the guidance, training and support for its implementation can be obtained from the NHS Connecting for Health (CFH) Clinical Safety Group.

John Fox, Senior Business Analyst, Quality & Safety
Email: john.fox1@nhs.net

The CFH Clinical Safety Helpdesk can be contacted to lodge support requests in respect of this standard:
Email: SafetyStandards@nhs.net

**Notes**:

1. Relevant organisations are those organisations as defined in the standard who must take direct action to implement the standard.
2. IT Suppliers are all suppliers to the organisations listed at 1 who supply functionality pertinent to that standard.
3. **Effective Date** is the date from which a new standard can be used but may not be mandatory. This might facilitate piloting, for example, or enable time for system functionality development. At this point, ***you "may use" the standard*.**
4. **Implementation Date** is the point from which the new standard becomes mandatory. Ideally, it inherently implies organisations use appropriate systems i.e. the date is the same for organisations and suppliers. However, there may be circumstances where interim workarounds are required i.e. the date is different for organisations and suppliers. At this date, ***you "must use" the standard***.
5. **Conformance Date** is the date from which the service and IT system suppliers must use the standard as envisaged i.e. using appropriate IT solutions rather than interim workarounds and, if the standard requires it, an independent, authoritative body or legitimate internal audit would conduct a conformity assessment with the expectation of full conformance by all relevant parties. It is the ***"must use standard effectively and assessed for use"*** date
6. **Superseded Date** of the prior standard sets the date at which the prior standard is replaced by the new standard i.e. the prior standard must no longer be used. This date will apply only where there was a pre-existing standard made redundant by the new standard. It might be different from preceding dates in the framework if, for example, a new and old standard run in parallel for a period. It is the date from which you ***"stop using the prior standard"***.