National review of clinical risk management standards DCB0129 and DCB0160

Public consultation

Help shape the future of patient safety

We are seeking views from manufacturers and users of health and social care technology products to help us improve the clinical risk management standards DCB0129 and DCB0160.

While we are keen to hear from wider audiences, this is primarily a technical consultation aimed at individuals with current experience or knowledge of the clinical risk management standards.

What are these standards and why do they matter?

These mandatory standards protect patients by ensuring all health IT systems (for example, electronic patient records and clinical decision support systems) are properly assessed for clinical risks before they are used in patient care. DCB0129 sets out requirements for technology manufacturers and DCB0160 covers how health and social care organisations deploy and use these systems safely.

Why are we reviewing these standards?

The revised standards must reflect advances in healthcare technology. For example, artificial intelligence supporting clinical decisions, complex interconnected systems sharing data across organisations, and new technologies like voice recognition and machine learning becoming routine in-patient care.

Before you begin

Participation in this consultation is voluntary, and all findings will be anonymised.

You must read the supporting information before answering the questions. This provides essential context about:

- our findings from focus groups with healthcare professionals, technology suppliers and clinical safety officers (CSOs)
- the current challenges

- the key areas we are considering for improvement

The questionnaire is divided into 3 sections

1. information about you (these questions require a response)
2. requirements established in the specifications (most of these questions require a response)
3. implementation guidance and wider support of the specifications (these questions are optional).

Please note it is likely that any changes made to the specifications will be in direct response to the analysis of the second set of questions.

To support individuals to consider their answers the full set of consultation questions are below. However, all responses must be submitted by completing the online consultation survey.

National review of clinical risk management standards DCB0129 and DCB0160: consultation questions

Section 1: About you

Q1. To help us understand the range of perspectives represented in this consultation, please provide the following information:

Which best describes your **primary** role? Select 1 option.

- clinical safety officer
- registered health or care professional (for example, registered clinician or social worker)
- non-registered health or care professional (for example, health or care manager or administrator)
- technology manufacturer or supplier
- clinical risk management professional
- safety engineer
- academic or researcher
- patient or service user representative
- national policy or strategy
- regulatory professional
- other (please specify)

Q2. Which sector do you **primarily** work in or with? Select 1 option.

- primary care (for example, GP practices, community pharmacies)
- secondary care (for example, hospitals, specialist services)
- community care services
- social care
- ambulance and emergency services
- mental health services
- independent healthcare

- technology industry
- academia or research
- national policy/strategy
- regulatory bodies
- other (please specify)

Q3. What is the approximate size of your organisation? Select 1 option.

- large (1000 or more employees)
- medium (250-999 employees)
- small (50-249 employees)
- micro (fewer than 50 employees)
- individual/freelance
- not applicable
- don't know

Q4. How many years of experience do you have working with DCB0129 and/or DCB0160 standards? Select 1 option.

- less than 1 year
- 1-3 years
- 4-7 years
- 8-15 years
- more than 15 years
- no direct experience with these standards

Section 2: DCB0129 and DCB0160 standards

Scope of the standards

We are keen to understand if the scope of the standards is adequate.

Q5. Should alternative risk management standards be adopted in health and adult social care in place of the current standards?

- yes (please suggest an alternative)
- no
- don't know

If you selected yes or no, please briefly explain your response in the text box below.

Q6. Do you think that DCB0129 and DCB0160 should apply to medical devices?

- yes
- no
- don't know

If you selected yes or no, please briefly explain your response in the text box below.

Q7. Do you think that the standards should include specific cybersecurity requirements for health IT systems?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Terminology

Exploring the precise language used within the clinical risk management standards will help ensure clarity and implementation.

We are keen to understand how we might improve the clarity of terms and definitions within the standards.

Q8. Are there specific definitions or terms within the current standards that require further clarification or updating?

- yes
- no
- don’t know

If you selected yes, please suggest specific improvements in the text box below.

Q9. The word ‘clinical’ is used extensively in the standards to contextualise risk management and digital clinical safety. Do you think the word should remain or be replaced?

- remain
- be replaced (please suggest an alternative)
- don’t know

If you selected remain or be replaced, please briefly explain your response in the text box below.

Risk-based classification and tiered approaches

We are keen to understand if the standards should adopt a risk-based approach.

Q10. Should the standards include different requirements based on the risk profile of the technology? (for example, a smaller subset of requirements is applicable to lower risk products)?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Clinical safety officers (CSOs)

CSOs are responsible for making sure that digital systems used in health and care are safe for patients. They review potential risks, ensure these are managed before systems are deployed and provide clinical sign-off that the technology can be used safely in practice.

Q11. Should the requirement for a CSO remain in the standards?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Q12. Does the CSO role need further definition?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Q13. Do you think the standards should include a defined supporting role to the CSO and clearer responsibilities for related roles?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Documentation and development practices

We are keen to understand whether the standards continue to align with current health IT systems developmental and deployment practices.

Q14. Do the mandated safety deliverables need revision in any way?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Q15. Should the standards accommodate modern development and deployment lifecycle practices (for example) agile methodologies?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Q16. Are all phases of a product lifecycle sufficiently addressed by the standards?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Review of existing requirements

The current DCB0129 and DCB0160 standards contain specific requirements that have been in place since 2009, with updates introduced in 2018.

We are keen to understand your views and if you believe there are requirements in the specification that should be amended, removed, or are missing.
If a text box is left blank, we will assume, for that question, you are satisfied with the requirements as currently expressed in the specification.

Q17. Requirements for **amendment**:
Which existing requirements should be modified and why? Please specify the requirement number (for example, DCB0129 requirement 2.3.1 or DCB0160 requirement 4.2.1) and your suggested revised text.

Open text response

Q18. Requirements for **removal**:
Are there requirements that should be deleted entirely? If so, please specify which ones (using requirement numbers) and explain your rationale.

Open text response

Q19. **Missing** requirements:
What new requirements should be added? Please specify which section they should go in and provide proposed requirement text.

Open text response

Section 3: Implementation guidance and wider system support (applicable to all health and care settings)

Patient safety

The focus groups generally felt that more could be done to align the standards to the wider work of patient safety teams. Despite the ambition of both standards being to improve patient safety, the work around the standards, digital clinical safety and overall patient safety sometimes felt disparate.

Q20. How could the standards and/or implementation guidance be better aligned to the broader effort to improve patient safety? Please also consider the role of clinical safety officers (CSOs).

Open text response

Professional development

The focus groups raised concerns that CSOs' skills and the support available to them vary across organisations. At the moment, a CSO must be a registered health or care professional (for example, a registered clinician or social worker). We are keen to understand whether there should be other ways to become a CSO.

Q21. Should alternative pathways be available for experienced non-registered health or care professionals to become CSOs? Select 1 option.

- yes, with additional clinical safety training
- yes, but requiring supervision by a registered health or care professional
- no, being a registered health or care professional should remain mandatory
- other (please specify requirements in the text box below)
- don't know

Please explain your reasoning in the text box below.

Q22. What are the minimum qualification requirements CSOs should have? Select all that apply, if any.

- current registration with appropriate professional body (UK based)
- current registration with appropriate professional body (globally based)
- formal qualification in risk management
- specific training and experience in healthcare technology and digital systems
- specific training and experience in patient safety
- demonstrated experience in clinical safety or risk management
- continuing professional development requirements
- other (please specify in the text box below)
- don't know

Please explain your reasoning in the text box below.

Q23. What support do CSOs need to be able to assure cyber security as part of the standards? Select all that apply, if any.

- training and guidance materials
- technical tools and templates
- access to cybersecurity expertise
- engagement with existing digital and cyber security teams
- clearer regulatory guidance
- other (please specify in the text box below)
- Don’t know

Please explain your reasoning in the text box below.

Q24. What other ongoing support do CSOs need most? Select all that apply, if any.

- professional development and training opportunities
- access to specialist technical expertise
- access to patient safety expertise
- peer support networks and communities of practice
- clearer guidance and templates
- protected time for safety activities
- senior leadership support within organisations
- other (please specify in the text box below)
- no ongoing support
- don’t know

Please explain your reasoning in the text box below.

Interoperability, integration and organisational accountability

Q25. Should the scope of the standards extend to interoperability and integration with third party systems?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Q26. Should the scope of the standards extend to include organisational accountability particularly in relation to risks that are transferable across systems?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Legacy systems

The focus groups expressed concern that some digital technologies used in healthcare are now very old and/or in regular use without proper adherence to the standards. These systems are often called ‘legacy’ systems.

Q27. How should legacy systems be managed? Select 1 option.

- treat them like new systems, with the same requirements and extended timelines for implementation
- use a risk-based approach to determine which standards apply
- create a separate pathway with specific requirements for legacy systems
- allow retrospective justification (‘proven in-use’) to reduce or modify requirements
- other (please specify)
- don’t know

Please explain your reasoning in the text box below.

Artificial intelligence (AI) and cybersecurity

The focus groups also identified that AI and cybersecurity are not adequately addressed.

We are keen to understand how to adapt the implementation guidance for these areas whilst maintaining patient safety as the priority.

Q28. Should the implementation guidance also extend to AI-enabled technology?

- yes
- no
- don’t know

If you selected yes or no, please briefly explain your response in the text box below.

Q29. How should the standards integrate with existing cybersecurity frameworks? Select all that apply, if any.

- require supplier’s NHS data security and protection toolkit status to be ‘standards met’ or ‘standards exceeded’
- completion of specific cybersecurity risk assessments as part of clinical safety assessments
- mandate certification to recognised cyber security schemes (for example, ISO27001, Cyber Essentials Plus etc.)
- align with National Cyber Security Centre guidance (not specific to healthcare)
- obtain assurance that the technical security criteria of the NHS digital technology assessment criteria are met
- other (please specify in the text box below)
- don’t know

Please explain your reasoning in the text box below.

Q30. Which cybersecurity risks require clinical assurance as part of the clinical risk management process? Select all that apply, if any.

- data breaches affecting the confidentiality of patient information (data is stolen and/or accessible to unauthorised parties)
- data breaches affecting the integrity of patient information (data is changed, accuracy is lost)
- data breaches affecting the availability of patient information (data cannot be accessed when needed)
- extended healthcare IT downtime (for example, server failure causing 2 days unavailability or a cyber-attack leading to 3 months unavailability)
- the impact of cyber-attacks affecting the healthcare IT system's supply chain (for example a third-party supplier's data centre used to host the system is impacted by an attack)
- third-party integration cyber security risks (for example, integration with other software introduces security weaknesses)
- other (please specify in the text box below)
- don't know

Please explain your reasoning in the text box below.

Q31. What should be considered when assuring the cyber security risk throughout the health IT system's full lifecycle? Select all that apply, if any.

- security of data throughout product lifecycle (including import at go-live/export at decommissioning)
- ongoing supplier/system cyber assurance processes
- processes for system maintenance/patching that require downtime
- plans for decommissioning/replacement of system ahead of vendor ceasing support
- ongoing management of system access and administration in line with good cyber hygiene practices
- other (please specify in the text box below)
- don't know

Please explain your reasoning in the text box below.

Innovation and safety balance

Some focus group participants highlighted that smaller, innovative companies may face particular challenges in complying with the standards while maintaining essential safety requirements.

Q32. How could the implementation guidance help organisations maintain compliance with the standards while also enabling innovation, particularly for smaller or emerging companies?

Open text response

Sector-specific implementation

The focus groups representing primary care, secondary care, community services, social care and ambulance services identified unique implementation challenges requiring tailored approaches. We are keen to explore sector-specific solutions to ensure the standards are applied consistently.

Q33. What are the key sector-specific challenges that need addressing in the implementation guidance?

Open text response

Q34. How could the implementation guidance better support smaller health and care organisations with limited resources, whilst maintaining safety requirements?

Open text response

Q35. How can the standards be more effectively applied across systems (for example, where similar technology may be deployed across multiple organisations)?

Open text response

Accessibility and inclusivity

It is essential that the clinical risk management standards ensure fair and equal protection for all patients. This means considering digital inclusion and accessibility and making sure safety assessments reflect the diverse needs of different patient groups. For example, technology such as pulse oximeters must work accurately and reliably across all skin tones.

Q36. Should clinical safety assessments explicitly include accessibility considerations? Select 1 option.

- yes, as mandatory requirements
- yes, as implementation guidance
- no, this is covered by other legislation
- other (please specify approach in the text box below)
- don’t know

Please explain your reasoning in the text box below.

Q37. To what extent, if at all, should patients and the public be informed or engaged in how digital health technologies are kept safe through the DCB0129 and DCB0160 standards? How could this be done effectively?

Open text response

Compliance and oversight

The focus groups consistently identified variations in compliance.

Building on this, we are keen to hear your views on how the standards can be applied more effectively and consistently across different health and care settings, and the kinds of support that would be most helpful for organisations. We would also like to explore with you how compliance could be encouraged and, over time, how approaches to oversight might be improved.

Q38. What specific support could be provided to help organisations achieve compliance? Select all that apply, if any.

- standardised templates and tools
- training programmes and workshops
- technical assistance and guidance
- peer mentoring networks
- sector-specific implementation guides
- certification of products or suppliers
- other (please specify in the text box below)
- don't know

Please explain your reasoning in the text box below.

Q39. What changes, or approaches would help your organisation (or the wider system) to apply the standards more effectively and consistently, and strengthen compliance and oversight over time?

Open text response

Future outlook

Q40. To what extent, if at all, should the standards be subject to regular review and updates?

Open text response

Q41. In your opinion, what else could be included as updates to the standards and/or implementation guidance to ensure comprehensive patient safety in the digital age?

Open text response

Thank you for your responses.