Caldicott2 Monitoring Reports - Further Information

Detail on the reports
The reports will pull through information on the following IG Toolkit requirements

- 101
- 200, 201, 202, 203, 205, 206
- 300, 302, 307
- 400

To enable the reporting some amendments have been made to requirements to reflect the Caldicott2 Report and the DH response as follows:

- New requirement statements for requirements 201, 202, 203 and 206.
- Amended attainment levels for requirements 200, 201, 202, 203, 205, 206 and 302.
- Additional guidance for requirements 101, 200, 201, 202, 203, 205, 206, 302 and 307.

Report presentation
The reports will be presented as status against the following Caldicott2 recommendations

- Recommendation 1 - 203, 205, 206
- Recommendation 2 - 201
- Recommendation 4 - 201
- Recommendation 5 - 302
- Recommendation 6 - 202, 302
- Recommendation 7 - 202, 203
- Recommendation 12 - 101, 200, 300, 307, 400
- Recommendation 15 - 101, 200, 300, 307, 400
- Recommendation 19 - 203

Reports will show the organisation:

- Has **fully implemented** a particular recommendation - all relevant IG Toolkit requirements within a recommendation are at level 3.
- Is **working towards** implementation of a particular recommendation - one or more IG Toolkit requirements within a recommendation are at level 1 or 2.
- Has **not started** implementing a particular recommendation - all relevant IG Toolkit requirements within a recommendation are at level 0.

PAGES 3 - 5 - TABLE SHOWING MAPPING OF CALDICOTT2 RECOMMENDATION TO IG TOOLKIT REQUIREMENTS

Mapping of recommendation to IG Toolkit requirements

Caldicott2 recommendation	Text of recommendation	IG Toolkit requirement(s)
Recommendation 1	People must have the fullest possible access to all the electronic care records about them, across the whole health and social care system, without charge. An audit trail that details anyone and everyone who has accessed a patient's record should be made available in a suitable form to patients via their personal health and social care records. The Department of Health and NHS Commissioning Board should drive a clear plan for implementation to ensure this happens as soon as possible.	**Patients/service users need to understand their rights** **203** - Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use. **There needs to be a subject access procedure in place that covers electronic records** **205** - There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data. **Systems must be capable of audit trails** **206** - Staff access to confidential personal information is monitored and audited. Where care records are held electronically, details about access to a record can be made available to the individual concerned on request.
Recommendation 2	For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual. Health and social care providers should audit their services against NICE Clinical Guideline 138, specifically against those quality statements concerned with sharing information for direct care	**Providers should ensure information is shared across organisational boundaries with those who are authorised** **201** - The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner.
Recommendation 4	Direct care is provided by health and social care staff working in multi-disciplinary care teams'. The Review Panel recommends that registered and regulated social workers be considered a part of the care team. Relevant information should be shared with members of the care team, when they have a legitimate relationship with the patient or service user. Providers must ensure that sharing is effective and safe. Commissioners must assure themselves	**Providers should ensure information is shared across organisational boundaries with those who are authorised** **201** - The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner.

	on providers' performance. Care teams may also contain staff that are not registered with a regulatory authority and yet undertake direct care. Health and social care provider organisations must ensure that robust combinations of safeguards are put in for these staff with regard to the processing of personal confidential data.	
Recommendation 5	In cases when there is a breach of personal confidential data, the data controller, the individual or organisation legally responsible for the data, must give a full explanation of the cause of the breach with the remedial action being undertaken and an apology to the person whose confidentiality has been breached	**The organisation must be able to identify and report breaches and attempts** **302** - There are documented information security incident / event reporting and management procedures that are accessible to all staff.
Recommendation 6	The processing of data without a legal basis, where one is required, must be reported to the board, or equivalent body of the health or social care organisation involved and dealt with as a data breach. There should be a standard severity scale for breaches agreed across the whole of the health and social care system. The board or equivalent body of each organisation in the health and social care system must publish all such data breaches. This should be in the quality report of NHS organisations, or as part of the annual report or performance report for non-NHS organisations.	**Staff need to be informed of what they can and cannot do with personal information** **202** - Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected. **The organisation must be able to identify and report breaches and attempts** **302** - There are documented information security incident / event reporting and management procedures that are accessible to all staff.
Recommendation 7	All organisations in the health and social care system should clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes. All organisations must also make clear what rights the individual has open to them, including any ability to actively dissent (i.e. withhold their consent).	**Staff need to be informed of what they can and cannot do with personal information** **202** - Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected. **Patients/service users need to understand their rights** **203** - Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use.
Recommendation 12	The boards or equivalent bodies in the NHS Commissioning Board, clinical commissioning groups,	**IG matters should be considered at the highest level of management in the organisation**

	Public Health England and local authorities must ensure that their organisation has due regard for information governance and adherence to its legal and statutory framework. An executive director at board level should be formally responsible for the organisation's standards of practice in information governance, and its performance should be described in the annual report or equivalent document. Boards should ensure that the organisation is competent in information governance practice, and assured of that through its risk management. This mirrors the arrangements required of provider trusts for some years	**101** - There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda. **Skilled personnel should be responsible for confidentiality and data protection** **200** - The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs. **Skilled personnel should be responsible for information security** **300** - The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs. **Skilled personnel should be responsible for information risk** **307** - An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy. **Skilled personnel should be responsible for information quality and records management** **400** - The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience.
Recommendation 15	The Department of Health should recommend that all organisations within the health and social care system which process personal confidential data, including but not limited to local authorities and social care providers as well as telephony and other virtual service providers, appoint a Caldicott Guardian and any information governance leaders required, and assure themselves of their continuous professional development	**IG matters should be considered at the highest level of management in the organisation** **101** - There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda. **Skilled personnel should be responsible for confidentiality and data protection** **200** - The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs. **Skilled personnel should be responsible for information**

		security **300** - The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs. **Skilled personnel should be responsible for information risk** **307** - An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy. **Skilled personnel should be responsible for information quality and records management** **400** - The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience.
Recommendation 19	All health and social care organisations must publish in a prominent and accessible form: • a description of the personal confidential data they disclose; • a description of the de-identified data they disclose on a limited basis; • who the disclosure is to; and • the purpose of the disclosure.	**Patients/service users need to understand their rights** **203** - Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use.