SAFE | WELL | PROSPEROUS | CONNECTED

Information Governance Framework

Schedule 03C

Caldicott Plan

IG Doc Ref – DOC NLC06	Review Date – November 2018	Version v2.3
This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website. Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.		

North Lincolnshire Council

Background Information	
Document Purpose and Subject	To provide a corporate Caldicott Plan.
Author	Information Governance Function.
Document Owner	Information Governance Function.
Last Review	January 2018
Current Review	November 2018
Change History	V2.3 - The policy has been updated to make reference to the General Data Protection Regulation and Data Protection Act 2018 that replaced the Data Protection Act 1998 on 25 May 2018.
File Location	Information Governance Shared Drive
Retention Period	Permanent Preservation as a Core Policy
Issue Date	04 January 2019
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	40 January 2019

Contents

1. Introduction

The Caldicott Guardian is a senior person within an organisation who acts as a conscience to protect the confidentiality of patient or social care service user identifiable information and to enable the appropriate sharing of this information. Above all the role is there to ensure the ethical use of this information. Additional guidance is available on the Gov.uk website - https://www.gov.uk/government/groups/uk-caldicott-guardian-council.

Caldicott is considered to be a key element of Information Governance and NHS organisations have been required to have a Caldicott Guardian and adopt the Calicott principles since 1998. This requirement was introduced into Local Authority social care in 2002 was mandated in England by the Local Authority Circular LAC(2002)2. It is considered good practice to adopt seven Caldicott Principles 26 recommendations. A third Caldicott review has taken place and when approved is expected to introduce principles about information security when sharing information.

Data Protection is the primary legislation underpinning Caldicott Guardian activities. The General Data Protection Regulation requires organisations to comply with six principles and the need to demonstrate accountability and compliance. There are close links and overlap between the General Data Protection Regulation and the Caldicott Principles.

North Lincolnshire Council has appointed Caldicott Guardians and this Plan outlines how we will comply with the principles and recommendations of Caldicott.

This plan is part of a suite of Information Governance and ICT policies and procedures.

2. Scope

This policy applies to all council employees and all individuals or organisations acting on behalf of the council and applies with patient or service user identifiable information is being processed.

3. Caldicott Reports

In 1997 a review was chaired by Dame Fiona Caldicott to ascertain how patient identifiable information was being handled in the NHS. The review made recommendations about the use and sharing of patient identifiable information in the NHS and six principles were highlighted, against which any release of health information should be justified. The recommendations were then expanded to cover social care service user identifiable information.

A second review was also chaired by Dame Caldicott during 2013 to look at the balance between the need to share patient or service user identifiable information and protecting confidentiality. This resulted in a report entitled 'Information: To share or not to share?' the addition of a seventh principle about information sharing and the addition of 26 recommendations. See appendix A for details of the recommendations.

In a speech to the NHS Innovation Expo in Manchester on 02 September 2015, the Secretary of State for Health challenged the NHS to make better use of technology. His proposals included rapid progress in the arrangements for patients to access and add to their own electronic health records. Technology will also permit health and social care professionals across England to share life-saving information about individuals, whenever and wherever they need attention. The Secretary of State said: 'Exciting though this all is, we will throw away these opportunities if the public do not believe they can trust us to look after their personal medical data securely. To address this issue, he commissioned a Review of data security and consent and asked for the Review to report in January 2016.

Firstly, he asked the Care Quality Commission (CQC) to review current approaches to data security across the NHS to prevent personal confidential data falling into the wrong hands. Secondly, he asked Dame Fiona Caldicott, the National Data Guardian (NDG), to develop data security standards that can be applied to the whole health and social care system and, with CQC, devise a method of testing compliance with the new standards. Thirdly, he asked Dame Fiona to propose a new consent/opt-out model for data sharing to enable people to make an informed decision about how their personal confidential data will be used.

4. Roles and Responsibilities

8.1 The key responsibilities of the Caldicott Guardian are to:

1. Strategy and Governance

- Represent patient and service user confidentiality and security issues at the Assurance Board within North Lincolnshire Council.
- Act as the 'conscience' of the council regarding confidentiality, and ensure that high standards are in place for the handling of patient and service user information, both within the council and for data flows to other organisations.
- Ensure that the Caldicott principles are reflected in the policies and procedures for the management and use of personal information.
- Support the Information Governance Function and Co-ordination role to develop and deliver Caldicott Guardian training and awareness.
- Support the Information Governance Function and Co-ordination role to produce a Caldicott Action Plan for the council.

- Carry out an annual Caldicott Review to check for ongoing compliance with the principles.
- Produce an annual report for the Management to provide an overview of the past year in relation to Caldicott and to report on compliance with the principles and any areas of concern.

2. Legal Framework

- Be aware of the legal framework governing the management of patient or service user identifiable information.
- In particular have an understanding of the following and how they work with the Caldicott principles:
    - General Data Protection Regulation and the Data Protection Act 2018 that should be considered alongside it, as the primary piece of legislation underpinning Caldicott Guardian activities.
    - The Common Law Duty of Confidentiality, which is made up from case law.
- To offer support and advice as required on matters relating to confidentiality and patient or service user information.

3. Internal Information Processing

- At a working level the Caldicott Guardian will to be consulted about individual cases where there are concerns about the potential disclosure of patient or service user identifiable information.
- To make the final decision, with support from the Information Governance Function and the Co-ordination role and Legal Services, if necessary, about issues that arise regarding the protection and use of or sharing of patient or service user personal information, noting that information can be shared when:
    - There is consent from the individual concerned and the individual has capacity;
    - Required by law;
    - In the public interest.

4. Information Sharing

- To support Managers, the Information Governance team and the Co-ordination role in the development of information sharing protocols and information sharing decisions.

5. Clinical Governance Link

- To bridge any gaps between Information Governance and Clinical Governance.

5. Caldicott Approval

Caldicott approval is required:

- If the release of patient or service user identifiable information is being considered in response to a request for information and there are concerns about release.
- If a new process is being considered that will collect, use or transfer patient or service user identifiable information.
- For information sharing agreements or data processing agreements where patient or service user identifiable information is to be shared, accessed or released.

6. Caldicott Principles

The 1997 and 2013 Caldicott reviews identify the following seven principles:

1. Justify the purpose for which the information is needed.
2. Only use information that identifies a patient or service user when absolutely necessary.
3. Use the minimum amount of patient or service user identifiable information.
4. That access to patient or service user identifiable information is only given to those who need it on a strict need to know basis.
5. That everyone with access to patient or service user identifiable information are aware of their responsibilities.
6. That the law is understood and complied with.
7. The duty to share personal confidential information being as important in some instances as the duty to respect service user confidentiality.

7. Caldicott Recommendations

See appendix A.

Appendix A – Recommendations from the Information Governance Caldicott Review 2013

No	Recommendation
01	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.
02	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.
03	The health and social care professional regulators must agree upon and publish the conditions under which regulated and registered professionals can rely on implied consent to share personal confidential data for direct care. Where appropriate, this should be done in consultation with the relevant Royal College. This process should be commissioned from the Professional Standards Authority.
04	Direct care is provided by health and social care staff working in multi-disciplinary 'care teams'. The Review 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 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 place for these staff with regard to the processing of personal confidential data.
05	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.

No	Recommendation
06	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.
07	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).
08	Consent is one way in which personal confidential data can be legally shared. In such situations people are entitled to have their consent decisions reliably recorded and available to be shared whenever appropriate, so their wishes can be respected. In this context, the Informatics Services Commissioning Group must develop or commission: • guidance for the reliable recording in the care record of any consent decision an individual makes in relation to sharing their personal confidential data; and • a strategy to ensure these consent decisions can be shared and provide assurance that the individual's wishes are respected.
09	The rights, pledges and duties relating to patient information set out in the NHS Constitution should be extended to cover the whole health and social care system.
10	The linkage of personal confidential data, which requires a legal basis, or data that has been de-identified, but still carries a high risk that it could be re-identified with reasonable effort, from more than one organisation for any purpose other than direct care should only be done in specialist, well-governed, independently scrutinised and accredited environments called 'accredited safe havens'. The Health and Social Care Information Centre must detail the attributes of an accredited safe haven in their code for processing confidential information, to which all public bodies must have regard. The Informatics Services Commissioning Group should advise the Secretary of State on granting accredited status, based on the data stewardship requirements in the Information Centre code, and subject to the publication of an independent external audit.

No	Recommendation

No	Recommendation
11	The Information Centre's code of practice should establish that an individual's existing right to object to their personal confidential data being shared, and to have that objection considered, applies to both current and future disclosures irrespective of whether they are mandated or permitted by statute. Both the criteria used to assess reasonable objections and the consistent application of those criteria should be reviewed on an ongoing basis.
12	The boards or equivalent bodies in the NHS Commissioning Board, clinical commissioning groups, 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.
13	The Secretary of State for Health should commission a task and finish group including but not limited to the Department of Health, Public Health England, Healthwatch England, providers and the Information Centre to determine whether the information governance issues in registries and public health functions outside health protection and cancer should be covered by specific health service regulations.
14	Regulatory, professional and educational bodies should ensure that: • information governance, and especially best practice on appropriate sharing, is a core competency of undergraduate training; and • information governance, appropriate sharing, sound record keeping and the importance of data quality are part of continuous professional development and are assessed as part of any professional revalidation process.
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.
16	Given the number of social welfare initiatives involving the creation or use of family records, the Review Panel recommends that such initiatives should be examined in detail from the perspective of Article 8 of the Human Rights Act. The Law Commission should consider including this in its forthcoming review of the data sharing between public bodies.
17	The NHS Commissioning Board, clinical commissioning groups and local authorities must ensure that health and social care services that offer virtual consultations and/or are dependent on medical devices for biometric monitoring are conforming to best practice with regard to

No	Recommendation
	information governance and will do so in the future.
18	The Department of Health and the Department for Education should jointly commission a task and finish group to develop and implement a single approach to recording information about 'the unborn' to enable integrated, safe and effective care through the optimum appropriate data sharing between health and social care professionals.
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.
20	The Department of Health should lead the development and implementation of a standard template that all health and social care organisations can use when creating data controller to data controller data sharing agreements. The template should ensure that agreements meet legal requirements and require minimum resources to implement.
21	The Health and Social Care Information Centre's Code of Practice for processing personal confidential data should adopt the standards and good practice guidance contained within this report.
22	The information governance advisory board to the Informatics Services Commissioning Group should ensure that the health and social care system adopts a single set of terms and definitions relating to information governance that both staff and the public can understand. These terms and definitions should begin with those set out in this document. All education, guidance and documents should use this terminology.

No	Recommendation
23	The health and social care system requires effective regulation to ensure the safe, effective, appropriate and legal sharing of personal confidential data. This process should be balanced and proportionate and utilise the existing and proposed duties within the health and social care system in England. The three minimum components of such a system would include: • a Memorandum of Understanding between the CQC and the ICO; • an annual data sharing report by the CQC and the ICO; and • an action plan agreed through the Informatics Services Commissioning Group on any remedial actions necessary to improve the situation shown to be deteriorating in the CQC-led annual 'data sharing' report.
24	The Review Panel recommends that the Secretary of State publicly supports the redress activities proposed by this review and promulgates actions to ensure that they are delivered.
25	The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the health and social care system.
26	The Secretary of State for Health should maintain oversight of the recommendations from the Information Governance Review and should publish an assessment of the implementation of those recommendations within 12 months of the publication of the review's final report.