CALDICOTT, CONFIDENTIALITY AND DATA PROTECTION POLICY

<table>
<thead>
<tr>
<th>Author:</th>
<th>Information Governance Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Director:</td>
<td>Richard Copland, Director of Health Information &amp; Technology</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Data approved:</td>
<td>January 2011</td>
</tr>
<tr>
<td>Date for Review:</td>
<td>January 2013</td>
</tr>
<tr>
<td>Version:</td>
<td>1.0</td>
</tr>
<tr>
<td>Replaces previous version:</td>
<td>0.2</td>
</tr>
</tbody>
</table>
## Contents

1.0 Introduction ..................................................................................................................3
2.0 Scope ...............................................................................................................................4
3.0 Roles and Responsibilities .............................................................................................4
   3.1 Role of Chief Executive ...............................................................................................4
   3.2 Role of Caldicott Guardian .........................................................................................4
   3.3 Role of Information Governance Manager ...............................................................4
   3.4 Role of Information Governance Steering Group ....................................................4
   3.5 Role of Directors and Heads of Departments ............................................................4
   3.6 Role of Staff ................................................................................................................4
4.0 Procedures ......................................................................................................................5
   4.1 Caldicott .......................................................................................................................5
   4.2 Confidentiality .............................................................................................................5
   4.3 Protecting Identifiable Information ...........................................................................5
   4.4 Informing Patients .....................................................................................................6
   4.5 Choice for Patients .....................................................................................................6
   4.6 Best Practice ...............................................................................................................6
   4.7 Data Protection Act ...................................................................................................6
5.0 Policy Review ..................................................................................................................7
6.0 Communication and Implementation ............................................................................7
7.0 Further Advice ...............................................................................................................7

Appendix A Caldicott Recommendations ............................................................................8
1.0 Introduction

Confidentiality is a fundamental principle in the delivery of health services. Much of the confidential information held relates to patients and employees of the service. This information should be treated with respect to ensure integrity, protect it from inappropriate disclosure and to make sure that it is only available to authorised staff. NHS Greater Glasgow & Clyde will take all reasonable measures to comply with its legal responsibilities and to preserve and maintain the confidentiality of the information it holds.

NHS Greater Glasgow & Clyde will ensure that all personal information relating to staff, patients or others will be treated in the strictest confidence and with due care and diligence at all times. This includes information held in manual or electronic format or information heard during the normal course of staff duties.

The purpose of this policy is to make staff aware of their obligations and duties in respect of the Caldicott Report 1997, the Duty of Confidentiality, and The Data Protection Act 1998.

This policy aims to clarify the principles which govern all uses of patient identifiable information.

Associated Legislation:

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Copyright, Design and Patents Act 1988
- The Access to Health Records Act 1990
- The RIP Act 2000
- The RIP(S) Act 2000
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Associated Policies and Standards:

- Information Governance Policy
- Clinical Communications Email Policy
- Email Acceptable Use Policy
- Internet Acceptable Use Policy
- Mobile Devices and Media Policy
- Information Technology Security Policy
2.0 Scope
This policy applies to all staff employed by NHS Greater Glasgow & Clyde. It also applies to contractors, partnership organisations and visitors not employed by NHS Greater Glasgow & Clyde but engaged to work with, or who have access to confidential, sensitive or personal identifiable information.

3.0 Roles and Responsibilities

3.1 Role of Chief Executive
The Chief Executive has overall responsibility for Data Protection. The Director of Health, Information and Technology has delegated functional responsibility for Data Protection.

3.2 Role of Caldicott Guardian
The Caldicott Guardian is the named individual within the Board who is responsible and accountable for the Board’s compliance with the Caldicott principles. This position is currently held by the Director of Health, Information and Technology and supported by the Boards Medical Director and Director of Public Health.

3.3 Role of Information Governance Manager
The Information Governance Manager has responsibility for advising staff on relevant legislation, policies and guidance procedures for information security across NHS Greater Glasgow & Clyde, reporting to the Caldicott Guardian and the Information Governance Steering Group, on confidentiality issues.

3.4 Role of Information Governance Steering Group
The Information Governance Steering Group will oversee the implementation of this agenda.

3.5 Role of Directors and Heads of Departments
Directors and Heads of Departments are responsible for ensuring that staff within their own directorates and departments work in a manner consistent with the principles outlined in the Policy.

3.6 Role of Staff
It is the responsibility of all staff to ensure they have read and understood this Policy and to ensure high standards of confidentiality are met.
4.0 Procedures

4.1 Caldicott

The Scottish Government is committed to implementing the recommendations of the Caldicott Committee’s Report on the Review of Patient-Identifiable Information.

The Report is based on six principles which ask us, when using patient identifiable information, to:

- Justify the purpose
- Use only when necessary
- Use the minimum necessary
- Access on a ‘need to know’ basis
- Be aware of your responsibilities
- Understand and comply with the law

One of the main recommendations of the Caldicott Report was the establishment of a network of Caldicott Guardians for patient information throughout the NHS. The full recommendations, which are being taken forward by NHS Boards, can be viewed in Appendix A.

4.2 Confidentiality

There are three basic rules for making a lawful disclosure of confidential information:

(i) where a person to whom the information relates has consented
(ii) where the disclosure is in the public interest
(iii) where there is a legal duty to do so (e.g. court order)

It is important that patients and staff are made aware of information disclosures which relate to them, in order to prevent a breach of confidentiality and to ensure compliance with the Data Protection Act.

4.3 Protecting Identifiable Information

For the protection of information:

- Staff, third party contractors, partner organisations and volunteers must be fully aware of their responsibilities regarding confidentiality. Advice should be sought from the Information Governance Manager in the first instance.
- The recording of information must be accurate and consistent
- Information is kept private
- Information is physically secure
- Appropriate care is taken when disclosing and using information
- Staff must not access any patient, employee or other record for which they have no proper reason to do so in the course of their duties
• Staff must not access records for their personal interest: this includes their own records.
• Staff should adhere to the NHS Code of Practice on Protecting Patient Confidentiality as set by the Scottish Government.

4.4 Informing Patients
Staff must inform patients:
• When information is to be recorded or their records accessed
• When they are disclosing information to others
• Of the choices available to them on how their information may be disclosed, and to ensure patients have no concerns about the disclosure
• On their rights when the patient wishes to access their health record

NHS Greater Glasgow & Clyde will ensure all new patients receive an information leaflet “Confidentiality and Your Health Records” before their appointment which will inform them how their information may be used.

4.5 Choice for Patients
Staff must provide choice to patients by:
• Asking patients before using their information in ways that do not directly impact on their delivery of care (e.g., teaching and research)
• Respecting patients’ wishes if they wish to restrict disclosure
• Informing patients of the implications to restricting disclosures

4.6 Best Practice
Staff must adhere to best practice by:
• Being aware of possible confidentiality issues
• Attend training sessions implemented by NHS Greater Glasgow & Clyde
• Seek support from the Information Governance Manager or the Caldicott Guardian when required
• Report possible breaches or risk of breaches to the Information Governance Manager

4.7 Data Protection Act

NHS Greater Glasgow & Clyde is required to collect and use a variety of sensitive and personal information about people in order to operate. This information includes data on past, current, and prospective employees, suppliers, patients/clients and others with whom it communicates. All personal information will be dealt with properly and securely no matter how it is collected, recorded and used – whether on paper, on computer or recorded on other material such as CCTV.

NHS Greater Glasgow & Clyde fully endorse and adheres to the principles of data protection as set out in the Data Protection Act 1998, namely that personal data:
• shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
• shall be obtained for only one or more specified and lawful purpose(s) and shall not be further processed in any manner incompatible with that purpose or these purposes;
• shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
• shall be accurate and, where necessary, kept up to date;
• shall not be kept for longer than is necessary for that purpose or those purposes;
• shall be processed in accordance with the rights of data subjects under the Act;
• that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data;
• shall not be transferred to a country or territory outside the European Economic Area\(^1\) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.0 Policy Review

This policy will be reviewed on an annual basis, unless the introduction of any new or amended relevant legislation warrants an earlier review.

6.0 Communication and Implementation

This Policy will be communicated through the Information Governance and IT Security Framework.

7.0 Further Advice

For further advice on this Policy please contact the Information Governance Manager.
Tel: 0141 211 1790 (x51790)
Email: Isobel.brown@ggc.scot.nhs.uk

\(^1\) Members of the European Union as well as Norway, Liechtenstein and Iceland
Appendix A

Caldicott Recommendations

1. **Information for Patients/Clients**
   The Board must have an active policy for informing patients of the kind of purposes for which information about them is collected and the categories of people or organisations to which information may need to be passed. Patients also need to be made aware of their rights, particularly their rights of access to their records.

2. **Code of Conduct**
   Staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

3. **Staff Induction Procedures**
   New staff should be provided with clear guidelines on their responsibilities in respect of confidentiality and security.

4. **Confidentiality and Security Training Needs**
   A regular and systematic assessment of training needs should be in place.

5. **Training Provision**
   This is linked with criteria 4, but looks more to the support that an organisation provides for its staff.

6. **Staff Contracts**
   NHS staff have a legal duty of confidence to patients and it should be made clear to them that breaching patient confidence can be a serious disciplinary offence. This can best be supported by the inclusion of a duty of confidence requirement in employment contracts or other documents setting out terms and conditions.

7. **Contracts Placed With Other Organisations**
   Where a non-NHS agency or individual is contracted to carry out or support NHS functions, the contract must specify appropriate confidentiality and security requirements.

8. **Reviewing Information Flows**
   Every flow of patient-identifiable information should be regularly justified and routinely tested against the Caldicott principles.

9. **Information/Data “Ownership”**
   It is best practice for each physical set of information (e.g., manual files or a database) to be assigned an “owner”.


10. Safe Haven Procedures
   Each organisation should establish safe-haven administrative arrangements to safeguard confidential person-identifiable information.

11. Protocols to Govern Information Sharing
   The transfer of all confidential person-identifiable information should be governed by clear and transparent protocols that satisfy the requirements of law and guidance and regulate working practices in both the disclosing and receiving organisations.

12. Security Policy
   An Information Security Policy should be in place which is reviewed and monitored on a regular basis.

13. Security Responsibilities
   An Information Security Officer should be appointed.

14. Risk Assessment and Management
   A risk assessment programme should be in place and regular reports available to senior management.

15. Security Incidents
   A system is in place to ensure that all security incidents involving the unauthorised disclosure of confidential personal information are reported to the Information Security Officer.

16. Security Monitoring
   Monitoring and reporting of security effectiveness should take place on a regular basis.

17. User Responsibilities
   A system should be developed whereby password changes are enforced on a regular basis.

18. Access Controls
   Organisations should have procedures and systems in place to control access to patient information and agreed responsibilities for who has access to what.