Document Details	
Title	Information Governance Policy
Author	Sue Barker
MP ref no:	IGP2
Version	3

Approval process	
Approved by	Middlewood Partnership Board
Date approved	10 March 2020
Document Category	Information Governance
Review Frequency	Annually

Distribution	
Who the policy will be distributed to?	All Middlewood Partnership Employees
Method	Middlewood Partnership Intradoc
Document Locator	'Intradoc', 'Documents', 'Policies', 'Information Governance'

Nominated Personnel (if applicable)
Caldicott Guardian: Dr Andrew Maurice IG Lead: Dr Paul Bowen Practice Manager at each site Data Protection Officer ('DPO'): Tara Moylan, GDPR Practitioner, who can be contacted at: Dpo.healthcare@nhs.net

Review		
Review date:	Reviewed by:	Brief details of amendments made:
26.11.20	Sue Barker	Extension of relevant 'information' to confidential information collected about 3rd parties by the Training Hub, update of DPO
15.3.20	Sue Barker	Addition of wording from PB re online consultation software (see Appendix 3), update of list of supporting policies (Appendix 2) and update of IG Lead
16.6.21	Laura Beresford	Update of IG lead.

Information Governance Policy

Contents

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

The Middlewood Partnership ("Middlewood") is committed to ensuring that information is effectively and efficiently managed, and that appropriate policies and procedures provide a robust framework for information management that is in full compliance with relevant legislation and guidelines. It is also committed to ensuring that there is sufficient management accountability to support the implementation of those policies and procedures.

2. Scope of this Document

This document is intended to provide to all staff a clear understanding of Middlewood's position with regards to information governance.

3. Awareness

Middlewood will take reasonable steps to ensure that staff are aware of this policy. The full policy is available on Intradoc, and staff are encouraged to speak to their Practice Manager or the IG Lead if they have any queries.

There are specific training requirements for staff, both during induction and on an annual basis, in relation to information governance. More details of this training are set out below.

4. Basic Principles

There are a number of sources of legislation and guidance that are applicable to the way that Middlewood manages the information it holds about its patients, staff and third parties including the Data Protection Act 2018 ('DPA') and the General Data Protection Regulation ('GDPR'). Middlewood has drafted its policies and procedures to take account of these.

The six basic principles of the DPA can be summarised as follows:

a) Personal data shall be processed fairly and lawfully;
b) Personal data shall be obtained and processed for specific lawful purposes, and will only be used for the purpose for which it was collected;
c) Personal data held must be adequate, relevant and not excessive;
d) Personal data must be accurate and kept up to date, and every reasonable step will be taken to ensure any personal data that is inaccurate is erased or rectified without delay;
e) Personal data shall not be kept for longer than necessary; and
f) Personal data shall be processed in a manner that ensures appropriate security of the personal data.

The National Data Guardian's (NDG) data security standards are set out in **Appendix 1**. Middlewood has committed to these standards and completes the annual Data Security and Protection Toolkit to demonstrate that it is meeting them.

Under their terms and conditions of employment, Middlewood staff may only access clinical information in the course of their normal duties and due to a genuine clinical or

administrative need. They are bound by a strict obligation of confidentiality. A breach of this obligation would be dealt with under the staff disciplinary policy.

5. Middlewood Information Governance Policies

Middlewood has a suite of policies that detail its collection, use, disclosure and disposal of information relating to patients, staff and third parties. These are saved onto the Middlewood Intradoc and reviewed annually. A list of current policies is set out in **Appendix 2**.

All Middlewood staff will refer to and comply with these policies, as appropriate.

6. Responsibilities of the Nominated Personnel and Middlewood Staff

The Caldicott Guardian has overall responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are a senior person who makes sure that information about those who use Middlewood services is handled legally, ethically and appropriately, and that confidentiality is maintained. The Caldicott Guardian will provide leadership and informed guidance on matters involving confidentiality and information sharing.

The IG Lead is responsible for:

a) Drafting and reviewing Middlewood's information governance policies;
b) Providing training and guidance to staff on the Middlewood information governance policies; and
c) Completing the annual Data Security and Protection Toolkit.

The Practice Manager is responsible for providing general support to staff in relation to information governance, and liaising with other Nominated Personnel, as appropriate.

The DPO is someone with experience of working with, and expert knowledge of, data protection law. Their role includes:

a) Informing and advising about compliance with the DPA and related data protection legislation;
b) Monitoring compliance with the legislation, including staff training;
c) Advising on and monitoring data protection impact assessments; and
d) Co-operating with the Information Commissioner's Office.

All Middlewood staff have a responsibility to safeguard the accuracy and security of the information that they collect and process during the course of their role.

7. Training

All new members of staff will receive training in information governance during their induction, and will be asked to complete an e-learning module during this period.

In addition, all staff will complete annual information governance training with a mandatory test that requires the achievement of 80% in order to pass.

The IG Lead will conduct spot checks throughout the year to gain an understanding of the levels of awareness amongst Middlewood staff of applicable policies and procedures. Any gaps that are highlighted through this process will be recorded, and action taken through newsletters, bespoke training and one-to-ones.

Any information governance learning points that are highlighted as part of the significant event analysis procedure will be incorporated into the training described above, as appropriate.

8. Records and Access Management

Middlewood has established and will maintain procedures for the effective management of records, following the principles listed in **Appendix 3**. Middlewood staff are expected to ensure effective records management within their area.

Where appropriate, Middlewood utilises the tools available in EMIS to pseudonymise data. This is particularly relevant to any projects with a research element. The pseudonymised data is kept separate to the identifying data, and is sufficiently independent of the identifying data so as to protect the patient's identity. Middlewood will ensure that in any information sharing agreements there is adequate protection in relation to pseudonymisation.

Middlewood maintains a log of all current staff, and their roles within the organisation. Each role has allocated systems access permissions.

APPENDIX 1 – Data Security Standards

1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
2	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3	All staff complete appropriate annual data security training and pass a mandatory test provided through the revised Information Governance Toolkit.
4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to sue workarounds which compromise data security.
6	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or near miss, with a report made to senior management within 12 hours of detection.
7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8	No unsupported operating systems, software or internet browsers are used within the IT estate.
9	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

APPENDIX 2 - List of Supporting Policies

- Access to Personnel Records Policy
- Clear Desk and Screen Policy
- Confidentiality and Data Protection Agreement for: Students, Foundation Drs and Trainees
- Confidentiality Policy
- Confidential Waste Disposal Policy
- Data Breach Policy
- Freedom of Information Act Policy
- Patient Privacy Notice
- Records Retention Schedule
- Requests to Access Health Records Policy
- Staff and Family Members as Patients Policy
- Staff Privacy Notice
- Visitors' Code of Conduct in Respect of Confidentiality

APPENDIX 3 – Principles of Records Management

Middlewood is committed to:

a) Developing the best practices for assessing and controlling data quality;
b) Ensuring continuous improvement of the processes, services and procedures for collecting, maintaining and recording data;
c) Communicating in a professional, open and transparent manner with all patients and partners;
d) Providing complete, accurate, appropriate, accessible and valid data in accordance with the General Data Protection Regulation 2016 and Data Protection Act 2018;
e) Providing and supporting professional development of staff members;
f) Optimising and effectively managing data by monitoring and managing the processes implemented in the Practice;
g) Ensuring the confidentiality and integrity of all physical and electronic data information;
h) Undertaking Data Protection Impact Assessments as appropriate; and
i) Providing adequate training for all employees of Middlewood on the issues of processing, recording and maintaining complete, accurate, accessible, appropriate and up-to-date data and keep employees aware of the importance of their personal contribution to it.

The following specific approach will be taken in relation to records management where Middlewood uses online consultation software:

When using online consultation software (e.g. AskmyGP, Accurx) to interact with patients, it is the responsibility of the clinician or staff member to copy, extract and paste relevant elements of the online conversation into the clinical record. This includes any documents or photographs shared. Third party software storage should not be considered part of the formal medical record, and as such, may be deleted or decommissioned meaning that any relevant consultation or clinical data could be lost. It is therefore important that any clinical information shard via an online or remote source is copied into the care record appropriately.

Equality Impact Assessment

		YES/NO	COMMENTS
1	Does the policy/guidance affect one group less or more favourably than another on the basis of;		
	• Race/ethnic or national origin/colour/nationality	No	
	• Disability	No	
	• Gender	No	
	• Religion / belief culture	No	
	• Sexual orientation	No	
	• Age	No	
	• Marital status	No	
	• Pregnancy or maternity	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are any exceptions valid, legal and/ or justifiable?	N/A	
4	Is the impact of the policy/ guidance likely to be negative?	No	
5	If so can the impact be avoided?	N/A	
6	What alternatives are there to achieving the policy/ guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	