Information Governance Policy

Version Control

Date	Version Number	Stage	Author
16th September 2014	1.0	Creation	Tim Crowson
3rd October 2014	2.0	Review and combining first draft with significant comments and drafting from Sister Sharon Leach	Paul Haycox
20th October 2014– inclusion of Caldicott information	Final Draft	Review and combining first draft with significant comments and drafting from Sister Sharon Leach	Paul Haycox
26th August 2016	Review	Review of policy in relation to organisation structure, changes in personnel and governance arrangements	Paul Haycox
19th January 2018	Review	Need further review against GDPR May 2018 when guidance available. Amended revised policy names, Removed response to 2013 guidance	Paul Haycox
24th May 2018	Review	Included elements around GDPR and Data Protection Act 2018	Paul Haycox
31st May 2019	Review	Minor update on syntax and on line training	Paul Haycox

Contents

1. Introduction

St Michael's Clinic Ltd. (STMC) is compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Good information governance and record management protects the rights and interests of patients, staff and members of the public who have dealings with STMC. It also helps the clinic to operate in an efficient and effective manner and ensures that it is operating in accordance with relevant laws and regulations.

This policy relates to the governance of all operational records. These are defined as information created or received during business and captured in a readable form, in any medium, providing evidence of the functions, activities and transactions of the clinic. They include:

- Administrative records, including personnel, estates, financial and accounting records, contracts and records associated with complaints.
- Patient health records including referrals, treatment records, correspondence with other health professionals, patient correspondence, out of licence drug records, treatment and chaperone registers.
- Photographs, imaging reports and images.
- Records in all electronic forms.

GDPR, Data Protection Act 2018 and Caldicott principles will always be observed and followed. Staff will receive training on these principles, relevant statutes and record keeping responsibilities. Clinical staff must follow professional guidelines on record keeping and confidentiality.

2. Purpose

The purpose of this document is to provide guidance, to all staff, on Information Governance.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements. There are a series of policies that relate to the Information Governance Policy :-

Information Governance Management Framework.

Information Risk management Policy

Confidentiality Policy

Data Protection Policy

Information Systems Security Policy

Document and Record Lifecycle Management Policy

Freedom of Information Policy

The aims of this document are:

a. To ensure that data is:

Held securely and confidentially.

Obtained fairly and lawfully.

Recorded accurately and reliably.

Used effectively and ethically

Shared and disclosed appropriately and lawfully.

b. To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, St Michael's Clinic Ltd. will ensure:

Information will be protected against unauthorised access.

Cybersecurity will be maintained at a reasonable and acceptable level

Confidentiality of information will be assured.

Integrity of information will be maintained.

Information will be supported by the highest quality data.

Regulatory and legislative requirements will be met.

Business continuity plans will be produced, maintained and tested.

Information governance training will be available to all staff, and all breaches of information governance, actual or suspected, will be reported to, and investigated by the Information Governance Senior Manager and reported to the Information Commissioners Office (ICO), if required.

3. Scope

All St Michael's Clinic Ltd. Staff which are within the Scope of this Document include:

Clinical Staff (Consultants, Doctors, Nurses and HCAs)

Administrative staff (Receptionists, Medical Secretaries, Administrative and technical staff

Staff working in or on behalf of St Michael's Clinic Ltd. (this includes contractors, temporary staff, secondees and any other permanent employees).

4. Roles and Responsibilities

Business Owner. Dr Stephen Murdoch as the clinical registered manager has overall accountability for establishing and maintaining an effective information governance regime and document management system, that meets all statutory requirements and adheres to guidance issued.

Caldicott Guardian. Dr Stephen Murdoch also acts as the Caldicott Guardian and will:

Strive to ensure the clinic meets the Caldicott principles as laid out in the 1997 review and the recommendations produced through the Information Governance review in March 2013 (see section on Caldicott Principles in Appendix 1)

Ensure that St Michael's Clinic Ltd. satisfies the highest practical standards for handling patient identifiable information.

Facilitate and enable appropriate information gathering

Represent and champion Information Governance requirements and issues at Senior Management level.

Ensure that confidentiality issues are part of the clinics policies, procedures and training for staff

Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the organisation.

Receive training as necessary to ensure they remain effective in their role as Caldicott Guardian

Senior Information Risk Owner (SIRO). The Business Manager has been nominated as Senior Information Risk Owner (SIRO), who will:

Take overall ownership of the organisation's Information Security Policy.

Act as champion for information risk.

Understand how St Michael's Clinic Ltd.'s business goals may be impacted by information risks, and how those risks may be managed.

Implement and lead Information Governance Risk Assessment and Management processes within St Michael's Clinic Ltd.

Advise the Senior Management Group on the effectiveness of information risk management within the organisation

Receive training as necessary to ensure they remain effective in their role as SIRO.

Information Governance Lead. The Information Governance Lead is the IT Manager, who will oversee all procedures affecting access to person-identifiable health data including:

Maintain an awareness of information governance issues within the organisation

Work with the Business manager to review and update the information governance policy in line with local and national requirements.

Undertake the role of Information Security Officer.

Review and audit procedures relating to this policy where appropriate on an ad-hoc basis, and

Ensure that line managers are aware of the requirements of the Information Governance policy

IT Manager. IT Manager is responsible for:

The formulation and implementation of IT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust IT security arrangements in line with best industry practice

Effective management and security of St Michael's Clinic Ltd. IT resources, for example, infrastructure and equipment

Ensure data is securely protected and safe from internal or external attack

Developing and implementing a robust IT Disaster Recovery Plan

Ensuring that IT security levels required by NHS Statement of Compliance are met

Ensuring the maintenance of all firewalls and secure access servers are always in place, and

Acting as the Information Asset Owner for the IT infrastructure with specific accountability for computer and telephone equipment and services that are operated

by corporate and clinical work force, e.g. personal computers, laptops, personal digital assistants and related computing devices.

Line Managers. Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their area.

All staff. It is the responsibility of each employee to adhere to the policy.

Staff will receive instruction and direction regarding the policy from several sources:

Policy and procedure manuals

Line manager

Specific training courses

Team meetings

Staff Intranet.

All staff are mandated to undertake appropriate Information Governance training annually.

All staff must make sure that they use the organisation's IT systems appropriately, and adhere to the Acceptable use of IT Policy.

All staff must adhere to all information security requirements and confidentiality as laid out in relevant policies.

5. Information Governance Policy Framework

The St Michael's Clinic Ltd. Information Governance Policy Framework is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with the NHS Operating Framework and the Data Security and Protection Toolkit requirements.

Policies. The Key Information Governance Policies are:

Data Protection Policy - *This policy sets out the roles and responsibilities for compliance with the GDPR and Data Protection Act 2018. Dr Stephen Murdoch is the named data controller for St Michael's Clinic Ltd. The clinic seeks to hold and process information in a transparent way and demonstrate compliance with the GDPR and Data Protection Act 2018.*

Data flows have been mapped and the legal basis for processing each data item logged. This is attached as an appendix to the Data Protection Policy.

The GDPR and Data Protection Act 2018 gives individuals the right to know what information is held about them and where is was gained from; the legal basis upon which that data is held; whether data is shared, processed or held by third parties; gives rights of individuals in relation to access to data held, correcting inaccuracies and have consideration of data being deleted. Individuals also have the right to expect their data to be kept securely. It provides a framework to ensure that personal information is handled properly.

All staff processing personal information must comply with the eight principles, which ensure that personal information is fairly and lawfully processed; processed for

limited purposes; adequate, relevant and not excessive; accurate and up to date; not kept for longer than necessary; processed in line with individuals' rights; secure and not transferred to other countries without adequate protection

Freedom of Information Policy - *This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.*

Confidentiality Policy - *This policy lays down the principles that must be observed by all who work within St Michael's Clinic Ltd. and have access to personal or confidential information. All staff must be aware of their responsibilities for safeguarding confidentiality, preserving information security and their contractual obligation through the confidentiality clause contained within their contracts of employment. All clinical staff must abide by their codes of professional conduct in relation to confidentiality, including the General Medical Council (GMC) Confidentiality guidance 2009; the GMC confidentiality guidance on protecting information 2009; the Nursing and Midwifery Council Code 2009, 2nd edition 2010 and review findings of July 2012. Information provided in confidence must not be used or disclosed in a form that might identify a patient without their consent*

Information Systems Security Policy - *This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation.*

Access to IT systems is controlled using secure log on and passwords and individual staff passwords. Backup data is held on a secure and remote hosted system. Physical access to areas where patient data or staff records are stored is by key pad - where the password is changed regularly and known only to staff. Out of hours the clinic has an alarm service that is linked to the police and fire departments. Remote access and use of portable devices are also covered within the policy.

Document, Record and Lifecycle Management Policy - *This policy is to promote the effective management and use of information. The clinic complies with the Records Management Code of Practice for Health and Social Care 2016*

Minimum retention periods may vary but St Michael's Clinic Ltd. adhere to the following minimum retention periods: -

- *Children and young people – until the patients 25th birthday, or 26th if the young person was 17 at the conclusion of treatment, or 8 years after the patient's death*
- *Health records – 8 years after last treatment or death*

When records are destroyed, paper records are shredded and electronic records either physically destroyed or permanently deleted.

Information Sharing Policy - *The policy will ensure that all information held or processed by St Michael's Clinic Ltd. is made available subject to appropriate protection of confidentiality and in line with the terms and conditions under which the data has been shared. This policy sets out what is required to ensure that fair and equal access to information can be provided and is supported by a range of procedures*

.

6. Clinical Governance Group

St Michael's Clinic Ltd. has a long established Clinical Governance Group and it has taken on the responsibility for Information Governance and Records Management. The group will monitor, and co-ordinate implementation of the Information Governance Policy and the Information Governance Toolkit (now the Data Security and Protection Toolkit) requirements and other information related legal obligations.

The group will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

Reviewing and signing off internal Information Governance policies and procedures.

Agreeing Information Governance awareness and training programmes for staff.

Ensuring compliance with Data Protection, Information Security and other information related legislation.

Providing advice and guidance on internal information governance to all staff.

Reviewing any data breaches (reportable and non-reportable) and overseeing any subsequent required actions. This responsibility is carried out through the SEA sub-group of the Clinical Governance Group and reports back to the main Group are made as necessary.

Providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO) for internal Information Governance related issues.

Ensure completion of the DSPT and receive a report on the outcome from completion

7. Distribution and Implementation of the policy

Distribution Plan

This document will be made available to all Staff.

A global notice will be sent to all Staff notifying them of the update of this document.

The document will be made available on a shared drive of the clinics intranet.

Training Plan

All staff are mandated to undertake appropriate Information Governance training annually.

An on line training package using Learning for Health is used for update training.

A training needs analysis will be undertaken with Staff when any major changes to policy is required.

8. Monitoring

Compliance with the policy will be monitored via the Clinical Governance group.

The Information Governance Manager is responsible for the monitoring, revision and updating of this document on a 2 yearly basis or sooner if the need arises.

9. Associated Documents

The following documents will provide additional information.

Freedom of Information Policy

Data Protection Policy

Confidentiality Policy

Document, Records and Lifecycle Management Policy

Information Systems Security Policy

Information Sharing Policy

Appendix 1

Caldicott Principles

CALDICOTT PRINCIPLES

The 1997 review of the uses of patient identifiable information by Dame Fiona Caldicott devised six general principles of information governance that could be used by all NHS organisations with access to patient information.

The Information Governance Review in March 2013 set out 26 recommendations, these are attached to this policy.

The Caldicott Principles on protecting patient information.

“Only those who are involved with the direct provision of care or with broader work concerned with the treatment or prevention of disease in a population should normally have access to patient identifiable information”

There was a revision of the Caldicott principles;

1. **Justify the purpose(s)**
   every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinized and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data.**
   where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis**
   only those individuals who need access to personal confidential data should have access to it, and they should only have access to data items that they need to see. This may mean introducing access controls or splitting data flows where one dataflow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**

Action should be taken to ensure that those handling personal confidential data- both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality.**

   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix 2

CALDICOTT RECOMMENDATIONS OF THE INFORMATION GOVERNANCE REVIEW 2013

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

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

Recommendation 3

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.

Recommendation 4

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.

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.

Recommendation 6 (section 4.6)

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.

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).

Recommendation 8

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.

Recommendation 9

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.

Recommendation 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.

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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

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.

Recommendation 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.

Recommendation 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 information governance and will do so in the future.

Recommendation 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.

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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

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.

Recommendation 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.

Recommendation 25

The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the health and social care system.

Recommendation 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.

Appendix 3

CALDICOTT GUARDIAN

The report recommends that a senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.

Dr. S. Murdoch is the Caldicott guardian for St Michael's Clinic Ltd., he will

- Ensure that STMC maintains the highest practical standards for handling patient identifiable information (PII)
- Facilitate and enable appropriate information sharing.
- Ensure that confidentiality issues are part of the clinic's policies, procedures and training for staff.
- Oversee all policies and procedures where confidential patient information is shared with bodies within and outside the NHS.