Information Governance & Data Security and Protection Policies

KINGSBRIDGE MEDICAL PRACTICE

Document Name	Information Governance
Version	1.0
Approved by	Glynis Croxon-Jones, Practice Manager
Approval Date	June 2020
Review Date	June 2021
Target Audience	All staff, including temporary staff and contractors, working for or on behalf of KINGSBRIDGE MEDICAL PRACTICE
Purpose	To set out the policy for Information Governance. To detail all staff responsibilities for Information Governance and the possible consequences of not following the guidance.

DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

Information Governance & Data Security and Protection Policies			
Version	**Valid From**	**Valid To**	**Document Path/Name**
1.0	**June 2020**	**June 2021**	**X:\GP Surgeries\Kingsbridge Medical\Information Governance\IG & GDPR\115 IG Policy**

Summary

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

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

The KINGSBRIDGE MEDICAL PRACTICE will establish and maintain this policy and the associated procedures to ensure compliance with the requirements contained in the Data and Security Protection Toolkit (DSPT).

This policy and its supporting procedures are fully endorsed by the Practice Management Team through the production of these documents and their endorsement and approval by the Information Governance Lead and Caldicott Guardian.

1. Scope

This policy covers all aspects of information within the organisation, including but not limited to:

- Patient/client/service user information
- Personal Information
- Organisational Information

This policy covers all aspects of handling information, including but not limited to:

- Structured record systems – paper and electronic
- Transmission of information – email, other forms of electronic transmission such as FTP, post and telephone

This policy covers all information systems purchased, developed and managed by or on behalf of the Practice, and any individual directly employed or otherwise working for the Practice.

The key component underpinning this policy is the annual improvement plan arising from a baseline assessment against the standards set out in the Data Security and Protection Toolkit.

This policy cannot be seen in isolation as information plays a key part in corporate governance, strategic risk, clinical governance, Caldicott principles, service planning, performance and business management.

The policy therefore links into all these aspects of the Practice and should be reflected in any respective strategies/policies.

2. Principles

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

All staff should read and sign the Staff Confidentiality Agreement and a copy should be retained on the staff record.

The Practice fully supports the principles of corporate and information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The Practice also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in the Practice to ensure and promote the quality of information and to actively use information in decision making processes.

The Practice will abide by the Caldicott Principles – these are listed in **Appendix A**, and the Data Protection Act 2018 principles – these are listed in **Appendix B**

There are 5 key interlinked strands to the Information Governance Policy:

- Openness
- Legal Compliance
- Information Security
- Records Management
- Data Quality

2.1 Openness

- The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Non-confidential information about the Practice and its services will be available to the public through a variety of media (e.g. leaflets, Internet, newsletter).
- The Practice regards all identifiable information relating to patients as confidential. Compliance with legal and regulatory framework will be achieved, monitored and maintained.
- The Practice regards all identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

- The Practice will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, Common Law Duty of Confidence, Freedom of Information Act 2000 and Environmental Information Regulations.
- The Practice will ensure that when personal identifiable information is shared, the sharing complies with the law, guidance and best practice and both service users' rights and the public interest are respected.
- Information Governance training including awareness and understanding of Caldicott principles and confidentiality, information security, records management and data protection will be mandatory for all staff. Information governance will be included in induction training for all new staff
- The Practice will undertake annual assessments and audits of its policies and arrangements for openness.
- Patients will have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Practice will have clear procedures and arrangements for handling queries from patients and the public.

2.2 Legal Compliance

- The Practice regards all person identifiable information, including that relating to patients as confidential.
- The Practice will undertake annual assessments and audits of its compliance with legal requirements.
- The Practice regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The practice will ensure that data is stored securely and processed in line with relevant legislation in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.
- The Practice will ensure compliance with the Data Protection Act 2018, Human Rights Act 1998 and the Common Law of Confidentiality and other relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

2.3 Information Security and Incident Reporting

- The Practice will undertake annual assessments and audits of its information and IT security arrangements through the Data Security and Protection Toolkit framework.
- The Practice will promote effective confidentiality and security procedures to its staff through policies, procedures and training.
- The Practice will ensure that data is stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share

information ensuring they comply with national and local requirements, policies and procedures

- The Practice will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- The Practice will log and record all reportable data security and protection incidents via the Data Security and Protection Toolkit reporting tool.
- The Practice will report a notifiable breach to the Information Commissioner's Office without undue delay, if longer than 72 hours then a specific reason for the delay will be given.

2.4 Records Management

- The Practice will undertake annual assessments and audits of its records management arrangements.
- The Practice will ensure that information is managed throughout its lifecycle of creation, retention, maintenance, use and disposal.
- The Practice will ensure that information is effectively managed so that it is accurate, up to date, secure, retrievable and available when required.
- All staff have a duty for the maintenance and protection of records they use. Only authorised staff should have access to records.
- The practice will identify and safeguard vital records necessary for business continuity and should include them in the business continuity /disaster recovery plans.
- The practice will record any incidents relating to records, including the unavailability and loss on the Data Security and Protection Toolkit.
- Accuracy of statements i.e. record keeping standards, should pay particular attention to stating facts not opinions.
- The practice will periodically check for records that have reached their minimum retention period and if there is no justification for continuing to hold them, they will be disposed of appropriately.

2.5 Data Quality

- It is the responsibility of all staff to ensure the information they generate is legible, complete, accurate, relevant, accessible and recorded in a timely manner. The quality of information produced can have a significant impact on the quality of services that we provide.
- The practice will ensure the quality of their records to the highest standards and wherever possible, information quality should be assured at the point of collection.

The practice will ensure:

- That all data must be correct and accurately reflect what happened. However, it is important to note that the accuracy and timeliness of data does not just relate to patients.
- That data will be within an agreed format which conforms to recognised national or local standards. Codes must map to national values and wherever possible, computer systems should be programmed to only accept valid entries.

- That data will be captured in full. All mandatory data items within a data set should be completed and default codes will only be used where appropriate, not as a substitute for real data.
- That data will be dealt with in a timely manner and should be collected at the earliest opportunity; recording of timely data is beneficial to the treatment of the patient. All data will be recorded to a deadline which will ensure that it meets national reporting and extract deadlines.
- That data collected should be understood by the staff collecting it and data items should be internally consistent. Data definitions should be reflected in procedure documents.
- That data will reflect the work of the Practice and not go unrecorded.
- That patients should not have duplicated or confused patient records, and where possible data should be recorded once, and staff should know exactly where to access the data. Where a duplicate record is created, for example in the event that a record is misplaced, records should be merged once the original is found.

3. Responsibilities

Glynis Croxon-Jones the designated Information Governance Lead in the Practice, is responsible for overseeing day to day Information Governance issues: developing and maintaining policies; standards, procedures and guidance; co-ordinating Information Governance in the Practice; raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the Information Governance responsibilities incumbent upon them and for ensuring that they comply with these on a day to day basis.

Dr Ayesha Hussain has been appointed as Caldicott Guardian for the Practice. This role is an amalgamation of management and clinical issues which helps to ensure the involvement of healthcare professionals in relation to achieving improved information governance compliance. The Caldicott Guardian has responsibility for ensuring that all staff comply with the Caldicott Principles and the guidance contained in the NHS Digital document – “A Guide to Confidentiality in Health and Social Care”.

The Caldicott Guardian will guide the Practice on confidentiality and protection issues relating to patient information. This role is pivotal in ensuring the balance between maintaining confidentiality standards and the delivery of patient care. The Caldicott Guardian will also advise the Practice Management Team on progress and major issues as they arise.

Hayley Gidman has been appointed as Data Protection Officer. The role will monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Full details of the roles and responsibilities for named individuals can be found in the document – Assignment of Responsibilities.

4. Training /Awareness

Information governance will be a part of the Practice's induction process. Records of all inductions will be retained on staff records.

All new and existing staff will receive annual mandatory training and guidance on information governance, which will include coverage of Caldicott and confidentiality, data protection, information security and Freedom of Information to ensure that staff are aware of their responsibilities for: the confidentiality of the information they handle; situations where it is appropriate to disclose information to persons other than the patient; safe haven procedures; quality record keeping; secure storage and disposal of information.

All staff must undertake the Data Security Awareness Level 1 e-learning module or equivalent training, and an assessment should be completed to demonstrate the required knowledge and understanding and to complete the training. This can be accessed through the E-Learning for Health website: https://www.e-lfh.org.uk/programmes/data-security-awareness

Annually all staff will complete Information Governance Refresher Training. Records of the staff compliance with training will be kept and monitored and the evidence from the training will be used to support the submission of the Data Security and Protection Toolkit.

5. Individual Rights

Individuals legally have rights in relation to the data that is processed about them. The Practice must have processes in place should an individual choose to exercise any of their rights. It is vital that all staff can recognise such requests to allow them to be processed within the timescales set out in law.

5.1 Subject Access Requests

The Practice will log and record all Subject Access Requests that are received in line with the Data Protection Act 2018.

A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Post
- Social media
- Practice website

Where an individual is unable to make a written request, it is the Department of Health's view that in serving the interest of patients it can be made verbally, with the details recorded on the individual's file.

All requests will be dealt with within one month, as per the legislation.

All information is to be supplied free of charge (although "reasonable" fees can be charged for an excessive request or for further copies).
A request may be received for information relating to a deceased individual. In this case certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:

• The patient's personal representative (Executor or Administrator of the deceased's estate)
• Any person who may have a claim arising out of the patient's death

A Next of Kin has no automatic right of access, but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from the Caldicott Guardian in relation to requests for deceased records.

The Common Law Duty of Confidentiality extends beyond death.

5.2 Right to erasure

The right to erasure is also known as 'the right to be forgotten' and means that individuals have the right to have personal data that the Practice holds about them erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- If the individual withdraws their consent for the Practice to process their data (if this was the basis on which it was collected).
- The personal data was unlawfully processed (i.e. a breach of UK data protection laws).
- The personal data has to be erased in order to comply with a legal obligation.

The Right to Erasure will be reviewed on a case by case basis and will be limited if the information has been processed for the purpose of providing direct care to the individual.

5.3 Right to be informed

Individuals have the right to be informed of the processing the Practice undertakes with their personal data. The Practice will information all individuals via their Privacy Notice.

The Privacy Notice is available on the Practice website https://kingsbridgemedicalpractice.co.uk/

5.4 Right to rectification

If personal data that the Practice holds is found to be inaccurate or incomplete, individuals have the right to have it rectified. This includes any data that the Practice may have passed on to others,

unless this proves impossible or involves disproportionate effort. If this is the case, the Practice will explain to the individual why this has not been possible.

The individual can make a request for rectification either verbally or in writing and the Practice has one calendar month to respond to such requests. The right to rectification is not absolute and the Practice has the right to review the request to see if it can be complied with.

Requests which are deemed to be unfounded, excessive, repetitive in nature or required to be maintained legally may be refused.

5.5 Right to restrict processing

Individuals have the right to restrict processing in certain situations. The data can still be retained by the Practice; however, certain restrictions can be applied.

The situations where processing restrictions may apply are:

- If the individual contests the accuracy of the data the Practice hold about them, the Practice will restrict the processing until the accuracy of the data has been verified;
- If the Practice is processing the individual's data as it is necessary for the performance of a public interest task and the individual has objected to the processing, the Practice will restrict processing while they consider whether their legitimate grounds for processing are overriding.;
- If the processing of the individual's personal data is found to be unlawful but they oppose erasure and request restriction instead; or
- If the Practice no longer need the data held about the individual, but the individual requires the data to establish, exercise or defend a legal claim.

Requests can be made verbally or in writing to the Practice and the Practice will respond within one month.

5.6 Right of data portability

Individuals have the right to request a copy of their data in a portable format if the processing of the personal data is on the legal basis of consent. If the personal data is being processed for the purpose of providing direct care to the individual, then this right will not apply.

5.7 Right to object

Individuals have the right to object to their data being processed if the data is being processed for the performance of a task in the public interest or exercise of official authority.

All objections will be reviewed on an individual basis and objections can be made to the Practice both verbally or in writing.

5.8 Right to object to automated decision making and profiling

Any information processed by the Practice which has been automated, meaning without human involvement will be eligible for this right.

The Practice does not currently use automated decision making or profiling tools.

6. National Data Opt-Out

All health and care organisations must comply with the national data opt-out policy by March 2020.

The Practice complies with the national data opt-out policy and the use of the technical services to check for national data opt-outs in line with technical specifications and instructions.

The Practice ensures that if patients do not wish for their confidential patient information to be used for research and planning, they can choose to opt out securely online or through a telephone service by contacting the practice directly. Further details are made available to the public via the Privacy Notice available to staff on the Kingsbridge Medical Practice shared drive and to the public via the website www.kingsbridgemedicalpractice.co.uk

7. Freedom of Information Requests

The Practice will deal with all Freedom of Information Requests (FOI) which are received in writing within 20 working days, in line with the Freedom of Information Act 2000.

Although requests will be treated along the lines of openness and transparency, some information may be exempt from release.

The Practice will review all requests and a Public Interest Test will be undertaken before the application of any exemptions for which this applies.

The Practice publication scheme can be found on the IG Compliance Manager toolkit.

8. Registration Authority

Smartcards are required to use and access IT systems essential to healthcare provision.

Individuals are granted access to a Smartcard by the organisation's Registration Authority lead. The Registration Authority Lead for the practice is Matthew Griffiths, Deputy Practice Manager.

The Registration Authority Team verify the identity of all healthcare staff who need to have access to patient identifiable or sensitive data. Individuals are granted access based on their work and their level of involvement in patient care.

The use of Smartcards leaves an audit trail.

Staff should be aware that disciplinary action may be taken if inappropriate action or unauthorised data access has been undertaken or Smartcards are shared.

9. Policy Approval

The Practice acknowledges that information is a valuable asset, therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders

This Policy has been fully endorsed by the formal approval of the Practice.

The Practice will, therefore, ensure that all staff, contractors and other relevant parties observe this policy in order to ensure compliance with Information Governance and contribute to the achievement of the Primary Care objectives and delivery of effective healthcare to the local population

10. Monitoring/Audit

- The Practice will monitor this Policy through Practice Management Meetings
- An assessment of compliance with requirements within the Data Security and Protection Toolkit will be undertaken each year.

To ensure that the Policy and other relevant Information Governance documents are being followed and implemented, Confidentiality Spot Check Audits will be undertaken throughout the financial year**.** These audits will identify any areas for improvement which can be provided to the Management team for implementation or risk assessed. Any risks which cannot be mitigated will be noted in the Business Continuity Plan.

11. Information Governance Management

Information Governance Management across the organisation will be co-ordinated by the Practice Management Team.

The responsibilities to the Practice Management Team will include, but not be limited to:

- Recommending for approval policies and procedures to be implemented within the Practice.
- Recommending for approval the annual submission of compliance with requirements in the Data Security and Protection Toolkit and related action plan.
- Co-ordinating and monitoring the Information Governance policy across the Practice.

The Practice Management Team will endorse the Information Governance policy for the Practice.

12. General Provisions

Non-Compliance

Non-compliance with this code of conduct by any person working for the Practice may result in disciplinary action being taken in accordance with the Practice's disciplinary procedure, a copy of which can be found in the Staff Handbook on the Kingsbridge Medical Practice Shared Drive.

13. Review

This policy will be reviewed on an annual basis or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health and/or NHS Executive.

- **Appendix A – Caldicott Principles**

The Caldicott Principles revised 2013 are:

Principle 1 - Justify the purpose(s) for using confidential information
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 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).

Principle 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.

Principle 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 the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 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.

Principle 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.

Principle 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 B – Data Protection Act 2018 Principles**

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It sits alongside the General Data Protection Regulation (EU) 2016/679 (GDPR), and tailors how the GDPR applies in the UK.

The GDPR sets out the key principles, rights and obligations for most processing of personal data and as a European Regulation, it has direct effect in UK law and automatically applies in the UK.

The Data Protection Act 2018/GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Article 5(1) requires that personal data shall be:
"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency'**);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('**purpose limitation'**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy'**);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation'**);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**')."

Article 5(2) adds that:
“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘**accountability’**).”