Policy No:	IG06
Version:	2.0

Name of Policy: Confidentiality and Data Protection Policy

Effective From: 13/01/2017

Date Ratified	29/09/2016
Ratified	QE Facilities Board
Review Date	01/09/2018
Sponsor	SIRO and Caldicott Guardian
Expiry Date	28/09/2021
Withdrawn Date	

Version Control

Version	Release	Author / Reviewer	Ratified by / Authorised by	Date	Changes (Please identify page no.)
1.0	13/01/2017	Lesley Jane/ IG Group	QE Facilities Board	29/09/2016	New Policy
2.0	1/9/2018	L Jane IG Manager		1/9/2018	Updated ref to GDPR Change title from Chief Executive to Managing Director Remove references to patient information where appropriate.

Contents

1. Introduction

QEF holds processes and shares personal data on a daily basis for various purposes during service provision.

All data must be treated securely and lawfully to deliver an effective services and to maintain confidence of its users. The current information security landscape and the legislative framework compels QEF to handle data that is in context with the components of the Information Governance Toolkit, the Department of Health (DoH) and Information Commissioner's Officer (ICO)'s guidelines and the legal obligations that arise from GDPR, the Common Law Duty of Confidentiality (including the NHS Confidentiality Code of Practice) and the Caldicott Principles.

2. Purpose

The purpose of this Policy is to:-

- Establish the principles of data handling for all staff;
- Promote how QEF will execute its duty to keep personal information safe and confidential whilst at the same time not compromising its ability to share information with other departments and partner agencies, where necessary;
- Provide assurance that QEF has full regard for the law and will only process information in order to provide the best possible care to its users;
- Establish a framework to provide assurance for the data protection and confidentiality components of QEF's Information Governance Toolkit;
- Ensure appropriate resources are allocated to QEF's training programme so that staff are adequately briefed.

3. Scope of this Policy

This Policy covers all QEF sites and applies to any individual employed, in any capacity, who is employed either under a letter of authority or on a permanent/part time or honorary contract or as a third party such as contractors, students, volunteers and visitors who handle information as part of their course of work.

The Policy covers all aspects of information within the organisation, including but is not limited to:-

- Service user/staff/client information;
- Personal information;
- Organisational information considered confidential or a trade secret;

It covers all aspects of handling information, including but not limited to:-

- Structured and unstructured record systems – paper and electronic;
- The transmission of information – fax, email, post and telephone;
- Photographic images, digital, text or video recordings including CCTV;
- Information held on mobile devices for e.g. Dictaphones, USB Memory sticks, laptops, tablets/IPADs, mobile phones and cameras etc.;
- Information systems managed and/or developed by or used by QEF;
- The purchase, development and maintenance of information systems in respect of the management of confidential/patient information.

This Policy will formally adopt the guidelines as set out in the Confidentiality: NHS Code of Practice (2003) set out by the Department of Health and the new superseded guidance "A Guide to

Confidentiality in Health and Social Care" recently published by the HSCIC in September 2013. QEF will observe the principles in these codes when making decisions regarding personal data.

4. Objectives of this Policy

The objectives of this Policy are to ensure that QEF will:-

- Publish (via Privacy Notices) and observe the conditions of fair and lawful processing so that staff and third parties are proactively informed of how their data will be used;
- Identify a legal justification for every data flow processed;
- Only use information for the purpose it was provided for unless exceptional circumstances permit where the public interest test prevails or an overriding legal statutory obligation exists that outweighs any patient confidentiality owed to a patient or client(s);
- Collect and process only information to the extent that it is needed to fulfil operational needs to comply with regulatory and statutory legal obligation(s);
- Ensure the accuracy and quality of the information used;
- Apply strict checks (i.e. retention periods) to the information it holds so that information is not held or kept for longer than necessary;
- Ensure that the rights of all data subjects are observed and actioned;
- Implement appropriate technical and organisational security measures to safeguard the use personal information; and
- Not transfer personal data abroad without adequate protection in place.

This Statement is in compliance with the principles of GDPR which includes the following rights for data subjects

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

5. The Information Handling Principles

QEF will:-

- Regard all personal identifiable data relating to patients, staff and business clients as confidential and will treat it with the respect it deserves by implementing an appropriate framework to achieve, monitor and maintain practice unless national policy on accountability and openness dictates otherwise;
- Establish appropriate procedures to ensure compliance with the GDPR, The Data Protection Act 2018, the Human Rights Act and the Common Law Duty of Confidentiality, Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and other related legislation;
- Ensure that staff who have a legitimate right of access as part of their duties are given authorisation to confidential information. Unauthorised access to personal data, regardless

of format i.e. electronic or paper, will be considered a breach of GDPR and will invoke staff disciplinary procedures, where this has been breached;

- Ensure staff only share information where it is appropriate to do so and where the transmission is secure and provides safe and effective care to individuals;
- Only make information disclosures where it is considered appropriate and is in respect of but not limited to:-
    - Auditing and assurance purposes for the improvement of quality care ;
    - The planning and management of services;
    - Risk management;
    - The investigation of complaints, notifications and legal enquiries/claims;
    - Legal statutory duties and requirements.
- Only use only identifiable information where it is only absolute necessary for a specified purpose in disclosure. The need for patients to be identified will be considered at each stage of satisfying the purpose(s). In all other cases anonymised data will be used to satisfy requests i.e. data will be stripped of its personal identifiers, where possible. Any sharing of anonymised data will specifically be for the benefit of the community or for a statutory duty;
- Ensure where the use of personal confidential data is considered essential, the inclusion of each individual item of data is justified so that only the minimum amount of personal confidential data is transferred or accessible as necessary for a given function to be carried out;
- Ensure all individuals have a legal right to object to the processing and sharing of their personal data, but any final decisions for disclosure will rest with QEF;
- Ensure individuals have a right to correct or delete data;
- Ensure every proposed use or transfer of personal confidential data within or from an organisation is clearly defined, scrutinised and documented with continuing uses regularly reviewed, by the appropriate Information Asset Owner, the Information Governance Manager, the SIRO and the Caldicott Guardian;
- Ensure staff are briefed on their roles and responsibilities so that they conform to the terms and conditions of their contract and understand their legal obligations when accessing confidential information;
- Ensure staff awareness is routinely assessed with appropriate training and informative communication;
- Conduct risk assessments, in conjunction with any planning of organisational activity where appropriate data protection privacy controls need to be determined and put into place.

QEF recognises that failure to adhere to these standards could form the basis of a complaint or legal claim. Staff are therefore required to take these necessary precautions when handling confidential data.

6. Staff and Management Responsibilities

Role	Description Role
Managing Director	The Managing Director has ultimate responsibility for compliance with QEF's data protection and confidentiality legal requirements. The implementation and compliance of this Policy is delegated to the SIRO, Caldicott Guardian, the Data Protection Officer and Information Governance Manager.
SIRO	The SIRO is assigned responsibility for the management of the suite of policies, procedures and processes associated with data protection and confidentiality and any escalating issues that materialises through QEFs Boards and Steering Groups.

Caldicott Guardian	The Caldicott Guardian will act as the conscience of the organisation in satisfying that QEF achieves the highest levels of standards for the handling of personal/confidential information and enabling appropriate information sharing controls and data flows to take place between all external and collaborative agencies. It is noted that QE Facilities does not process health information. The Caldicott Guardian will play a key role in: • Ensuring there is a framework for enabling the Caldicott principles to be reflected in QEF's policies and procedures; (note at present QEF does not share patient information) • Supporting data sharing agreements; • Championing QEF's confidentiality and information sharing requirements and issues at Board Level with the SIRO.
Data Protection Officer (Facilities Manager – Security)	The Data Protection Officer will: • Develop and implement the Confidentiality and Data Protection Policy; • Provide information and guidance on the processing of all personal data; • Produce 'best practice' guidance material for staff • Deliver training to staff; • Process, co-ordinate and respond to all requests for information (with support from GHNT as part of the Service Specification); • Receive and consider reports into data breaches of confidentiality and where appropriate undertake, recommend or sign off necessary remedial action
IG Manager	The IG Manager will:- • Ensure QEF has an effective management framework of policies and arrangements to cover all aspects of data protection, confidentiality, data security and information governance; • Advise the governing body on all issues in relation to data protection and confidentiality and agree the appropriate components/controls for the IG Toolkit sign off; • Ensure QEF's information handling practices for keeping information secure and respecting confidentiality of staff and service users is maintained and communicated to employees; • Ensure QEF undertakes or commissions appropriate annual assessments and audits on its IG framework to determine current arrangements are adequate; • Ensure there is an IG Improvement Plan in place that secures the necessary implementation of resources and monitors progress of the plan; • Support QEF's Caldicott Guardian, Senior Information Risk Officer (SIRO) and Data Protection Officer with their data protection and data security functions; • Advise on all matters relating to staff training, the

	investigation of actual and near miss security incidents / breaches, audit studies and any data sharing compliance needs.
Information Asset Owners (IAOs) (i.e. Heads of Services)	All IAO's will assume responsibility for the information assets they hold (paper and electronic) and ensure robust, adequate and compliant procedures are in place for the handling of personal, sensitive or commercial information. Each IAO will ensure:- • All current and future staff are instructed on their duty of confidentiality and security legal obligations and are kept up to date with policy & procedure changes; this should be performed during induction and refreshed at least annually or when changes to legislation occur; • Staff abide by QEFs Caldicott and Safe Haven Procedure and IT and Information Security Policy when sending PID in and out of QEF; • All system access to IT systems is based on job function only, independent of status to prevent any unauthorised data breaches; • That relevant system administrators/managers are advised of staff changes (i.e. starters and leavers) and where passwords need to be disabled; • Regular spot checks are undertaken in their service area to ensure QEF's data flows are not susceptible to a data breach; • All new systems, processes and services which hold or process personal data are subject to the ICO's Privacy Impact Assessment Code of Practice.
Information Asset Administrators (IAAs) (i.e. Managers / Supervisors)	All IAAs will assume responsibility for compliance with GDPR, this Policy and the information assets for which they have been nominated by the IAO. The IAA will also be responsible for ensuring that the information asset is audited before implementation and is regularly risk assessed at least annually. These audits will require approval by the IAO.
All Staff	All staff, and anyone working on behalf of QEF, involved in the receipt, handling or communication of person identifiable data will adhere to this policy. Staff must observe:- • QEFs guidance and procedures in relation to the obtaining, use, disclosure and disposal of personal data. • Terms and conditions of their employment contracts. Staff are therefore expected to familiarise themselves with this Policy so that they understand their legal obligations and do not make any unauthorised disclosures to third parties.

7. Definitions

7.1 General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.

In general terms, this gives individuals a legal right to:-

- Privacy;
- To know the purposes for which their data is held and processed;
- To have data corrected or deleted;
- To know who their data may be disclosed to or shared with; and
- To prevent the use of their data in certain circumstances.

The underlying aim of GDPR is to:-

- Promote openness about the processing of people's personal data; and
- To ensure information relating to an individual is treated as confidential and is not communicated to anyone who is not authorised to receive it. Unauthorised persons including staff not involved in either the clinical care of a patient or the associated administration process. In the case of staff records, unauthorised persons including staff not involved in the management of that member of staff or associated administrative processes.

For deceased individuals a duty of confidence still continues.

Key areas of change:-

Breach Notification – Data Breaches will be reported via the Trusts Risk Reporting system (DATIX) and it is noted that potential fines will now increase to a maximum of 20 million euros (equivalent sterling at the exchange rate on the day the fine is issued). The requirement is for breaches to be reported within 72 hours.

Individuals Rights – Individuals have greater rights under the General Data Protection Regulation including the right of access, right to rectification, right to erasure (right to be forgotten), right to restriction of processing, right to data portability and the right to object. These rights will be considered by QE Facilities when in receipt of an application.

Contractual Requirements – The GDPR requires all third parties who process data on behalf of the QE Facilities to comply with relevant contractual provisions. The provisions are detailed in the Information Governance Policy for new Systems and changes to existing Systems.

Privacy Impact Assessments (PIAs) – The use of Privacy Impact Assessments is a statutory requirement under the General Data Protection Regulation for all fundamental changes in the way that personal data is stored, transferred and used.

Changes to Subject Access Requests - Key changes to subject access requests include the timescale is now one month to respond and charging has been removed. Further detail is contained within the Subject Access Request Policy.

Employment Contracts – Information Governance provisions within contracts and employment handbooks will be updated to include the relevant provision.

Privacy Notices/Fair Processing Notices – All privacy information will include the provisions of the new General Data Protection Regulation. This includes information on the identity and contact details of the controller, purpose and legal basis, recipient or categories of recipient, retention periods and the right to withdraw consent (if applicable).

Information Asset Register/Data Flow Maps – There is a statutory requirement under the GDPR to ensure that the there is a record of data processing activities which will be maintained and updated by the Information Governance Team.

7.2 Data Protection Act 2018

The Data Protection Act 2018 will make provision for the processing of personal data and states that "most processing of personal data is subject to the GDPR".

Data Protection Act 2018 Principles:-

Principle 1 - Processing of personal data must be (a) lawful and (b) fair and transparent.

Principle 2 - (a) the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected

Principle 3 - Personal data must be adequate relevant and not excessive in relation to the purpose for which it is processed

Principle 4 - Personal data undergoing processing must be accurate and where necessary kept up to date

Principle 5 - Personal data must be kept for no longer than is necessary for the purpose for which it processed

Principle 6 - Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data

Definition of Personal Data

The definition of personal data under Article 4 of the General Data Protection Regulation is defined as follows:-

"personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name an identification number location data an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The definition of sensitive personal data is as follows under Article 9 with regards the processing of special categories of personal data:-

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation shall be prohibited.

7.3 Caldicott Principles

- Justify the Purpose
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data

- Access to personal confidential data should be on a strict need to know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Understand and comply with the law

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

7.4 Common Law Duty of Confidentiality

The Common Law Duty of Confidentiality prohibits use and disclosure of information, provided in confidence unless there is a statutory court order or requirement to do so. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest for example to protect the vital interests of the data subjects or another person or for the prevention or detection of a serious crime.

7.5 Confidentiality and Data Protection

QE Facilities will:-

Regard all personal identifiable data relating to patients, staff and business clients as confidential and will treat it with the respect it deserves by implementing an appropriate framework to achieve, monitor and maintain practice unless national policy on accountability and openness dictates otherwise;

Ensure that staff who have a legitimate right of access as part of their duties are given authorisation to confidential information. Unauthorised access to personal data, regardless of format i.e. electronic or paper, will be considered a breach of the Data Protection Act and will invoke staff disciplinary procedures, where this has been breached;

Ensure staff only share information where it is appropriate to do so and where the transmission is secure and provides safe and effective care to individuals;

Only use only personal identifiable data where it is necessary for a specific purpose. The need for patients to be identified will be considered at each stage of satisfying the purpose(s). All who work for QEF will observe their own behaviour and the following standards of this Policy . Such obligations to confidentiality will include but not limited to:-

- Not gossiping or uploading confidential statements or posts involving staff, patients and suppliers onto social media, blogs or forum websites without consent etc;
- Not making inaccurate libellous, defamatory, harassment, threatening statements that may otherwise be illegal or which could bring QEF into disrepute;
- Not leaving systems logged on so that other staff members can access IT systems. All logins will be locked down or closed down when not in active use;
- Not leaving storage areas/rooms unlocked or not conforming to health and safety requirements for flood, theft, fire and environmental damage;
- Ensuring computer screens and whiteboards that contain personal confidential data (PCD) are not visible in public areas, especially in reception areas;
- Not using personal data for secondary purposes for e.g. research and development purposes without consent;
- Adhering to QEF wide and local procedures. This covering but not limited to:-.
    - The Caldicott Safe haven procedure for guidance on the transfer of personal data using fax machines, emails, and post (internal and external);
    - The protocol for dealing with telephone calls and leaving messages on patients/employees mobiles and answer machines;

- The destruction and disposal of confidential waste/removable media;
- The use of NHSnet mail for emailing patient or personal identifiable data to external agencies;
- The restrictions on access to secure areas;
- The protocol for transferring and signing in and out personal/patient information;

8. Policy

8.1 Breaches of Confidentiality

All breaches of confidentiality must be reported via the Trusts DATIX reporting system and will be investigated to determine the seriousness of the breach and any associated action that is required. Incidents can include but are not limited to:-

- Unlawful disclosure of personal or sensitive data ;
- Inappropriate direct access healthcare or personal information relating to individuals where there is no direct care relation e.g. friends, family, acquaintances, celebrities;
- Sharing of passwords and smartcards where the person has not been given authorised access;
- The accidental disclosure of staff or patient information to third parties.

8.2 New Systems, Processes and Services

Before procurement or development of new systems/processes/services staff should refer to the Information Governance Policy for new Systems and changes to existing Systems which details a three stage approach. This includes:-

- Initial screening questions for a Privacy Impact Assessment (PIA) and the completion of a full where required
- New systems and service providers should complete the screening questions as appropriate (additional screening questions for IT systems)
- All organisations who have access to QE Facilities data must sign up to the relevant terms and conditions required as a data processor under UK Data Protection legislation.

8.3 IT Security

Gateshead Health NHS Foundation Trust hosts the network and server architecture on behalf of QE Facilities. The Trust will ensure that it meets the required standard in the Data Security and Protection Toolkit which encompasses Cyber Security elements e.g. Patching, Anti-Virus and Malware Protection. The Trusts approach to cyber security is further detailed in their IT and Information Security Policy.

9 IT/Systems Testing

The use of personal identifiable data will be avoided for system testing. Where there is no practical alternative to using live data sign off will be required by the SIRO.

10. Training

All staff are required to undertake annual Information Governance Training which will encompass the key requirements including Data Protection and the Common Law Duty of Confidentiality.

11. Equality and Diversity

QE Facilities is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat staff reflects their individual needs and does not unlawfully discriminate against individuals or groups on the grounds of any protected characteristic (Equality Act 2010). This policy aims to uphold the right of all staff to be treated fairly and consistently and adopts a human rights approach. This policy has been appropriately assessed.

"An equality analysis has been undertaken for this policy, in accordance with the Equality Act (2010)."

12. Monitoring and Compliance

Compliance with this Policy will be undertaken by the Information Governance Lead in the following manner:-

Standard / process / issue	Monitoring and Audit			
	Method	**By**	**Group/Committee**	**Frequency**
Compliance with this Policy	Monitoring and investigation of IG/Data Confidentiality DATIX related incidents	IG Manager	IG Group	Quarterly
	Spot checks carried out to check procedures are being followed	IAO/IAA IG Manager	IG Group	Annually
Staff training	The monitoring of staff attendance to training sessions	IG Manager/IAO	IG Group	Quarterly
Compliance with the IG Toolkit	The score of the IGTK in the Data Protection and Confidentiality components	IG Manager	QEF Board	Annually

13.0 Disclosures with Respect to the Law

13.1 Permitted Disclosures

There may be occasions when QEF is bound to make a disclosure without consent.
Information disclosures made under statue include:-

- Poisonings and serious accidents in the work place;
- Serious road traffic accidents;
- The prevention/detection of a serious crime i.e. terrorism, murder, GBH etc.

13.2 Permitted Disclosures without Consent

Although rare, there may be occasions when patient confidentiality may be overridden following consultation with either senior management or a senior clinician lead. This includes but is not limited to:-

- There is serious danger to people and the right to patient confidentiality is superseded by the need to protect others for e.g. there is a serious threat to QEF, to a health care or admin professional;
- There is a serious threat to national security or to the local community e.g. terrorism;
- There is a legal obligation to make a disclosure in respect of a Court Order or a s29(3) request in respect of a serious crime, taxation or fraud enquiry by either the Police of a Government Body e.g. HMRC or DWP;
- To pursue the discharge of QEF's regulatory functions (e.g. safety and welfare of people at work);
- In other circumstances, based on professional consideration and consultation

QEF will always observe the principle of proportionality when serving the public good.

14.0 Disclosures Unrelated to Healthcare or Other Medical / Statutory Purposes

There are a number of other situations where QEF would be expected to make an information disclosure without the person's consent. Such examples include:-

- Government departments (excluding the Department of Health for Healthcare purposes) e.g. DWP, HMRC conducting fraud investigations etc;
- The Police;
- Acting Agents and Solicitors;
- Non-statutory investigations, e.g. Members of Parliament;
- The courts, including a coroner's court, tribunals and enquiries.

15.0 Disclosures for Non-Healthcare Secondary Purposes

Patient personal data for non-healthcare purposes may be disclosed for:

- Service evaluations / complaints process.

16.0 Processing Information

16.1 Data Sharing Agreements

Any routine sharing of personal/patient information between professional and organisational boundaries such as the Local Authorities, the Police etc. will be covered by formal data sharing agreements. The agreement will underpin the formal arrangements and document the detail of what is to be shared, why, with whom and any other house-keeping arrangements (for e.g. security controls for data transfer, media interest, the handling of complaints and information requests etc.)

All data sharing agreements will be reviewed by the IG Manager and signed off by QEF's Caldicott Guardian and/or SIRO.

16.2 Third Party Contractors

Any contractors commissioned on behalf of QEF that have access to personal data will be required to sign formal confidentiality agreements to ensure they have the appropriate security arrangements in place and do not compromise QEF's data protection legal requirements.

17 Consultation and Review

This Policy will be reviewed on a two year basis unless subject to legislative or case law changes or any changes or releases in NHS good practices or where deficiencies of information risks have been identified following the report of a significant data security incident

18 Associated Policies and Documentation

This Policy is part of a suite of supporting Information Governance related policies that sets out QEF's standards for those who work with personal or confidential data on a day to day basis. Further guidance can be sought from the policies stipulated below:-

- Freedom of Information Policy
- Information Security Policy
- Records Management Policy
- Subject Access Request Policy
- Information Governance Policy for new Systems and changes to existing Systems
- Data Protection Procedure
- Caldicott and Safe Haven Procedure
- Staff Confidentiality Code of Conduct

19 References

- General Data Protection Regulation
- Data Protection Act 2018
- Common law duty of confidentiality
- Freedom of Information Act 2000

Information Acts

- GDPR and Data Protection Act 2018;
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998);
- Health and Social Care Act 2012;
- The Human Rights Act (HRA) 1998 (Article 8);
- The Access to Health Records (NI) Order 1993;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Protection of Freedoms Act 2012;
- Public Records Act 1958;
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000);
- Common law related to the duty of confidentiality;
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992;
- Electronic Communications Act 2000;
- Audit & Internal Control Act 1987.

Crime Acts

- Crime and Disorder Act 1998;
- Police and Criminal Evidence Act 1984;
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000;
- Road Traffic Act 1988;
- Coroners and Justice Act 2009;
- Public Interest Disclosure Act 1998.