Data Security and Protection Policy

(previously Information Governance Policy)

Pragmatic Clinical Trials Unit (PCTU)

Policy number	PCTU_POL_IG_01	Version number	5.0
Publication date	29 March 2019	Review date	28 March 2019

Author:	Arouna Woukeu
Reviewed by:	Sandra Eldridge, Ann Thomson, Sarah Elaine Thomas, Sally Kerry, Anitha Manivannan, Tahera Hussain

Authorisation:	
Name / Position	Arouna Woukeu - PCTU Information Governance Lead
Signature	*Pdf version with signature on shared drive*
Date	29 March 2019

Contents

1. Introduction

Information is a vital asset, in terms of running clinical studies, meeting the strategic objectives of the Pragmatic Clinical Trials Unit, and the efficient management of services and resources within the unit. It plays a key part in service planning, service delivery and performance management. It is therefore of paramount importance that information is efficiently managed and that appropriate policies, procedures, management accountability and structures are implemented for a robust governance framework of information management.

Data Security and Protection provides a way for employees to deal consistently with the different pieces of legislation about how data is handled such as The Data Protection Act, The Common Law Duty of Confidentiality, The Freedom of Information Act and the General Data Protection Regulation.

NHS digital is commissioned by the Department of Health and Social Care to develop and maintain rules, policies and guidance regarding information governance and data security and protection that all Health and Social Care service providers, commissioners and suppliers need to comply with.

The Department of Health and Social Care policy states that all organisations that have access to and process NHS patient data, for whatever purpose, are required to provide assurances that they are practicing good information governance and data security and protection practices.

The Data Security and Protection (DSP) Toolkit is an online tool that enables relevant organisations to measure their compliance with the data security and information governance requirements mandated by the Department of Health and Social Care.

The DSP Toolkit replaces the IG Toolkit in providing the mechanism for organisations to carry out this assessment and to demonstrate that they can be trusted to maintain the confidentiality and security of personal information.

The DSP Toolkit was developed in response to The National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs published in July 2016 and the government response published in July 2017.

.

The Pragmatic Clinical Trials Unit uses the framework of the DSP Toolkit [reference 1.1]to ensure a process of continuous quality improvement in relation to information governance within the unit.

Definitions
Data (or Information) in the context of this Policy includes all research and business related data held in an electronic or other format by the Pragmatic Clinical Trials Unit (PCTU) including, but not exclusively, about study participants, staff, third party service providers,

Standard Operating Procedures (SOPs), risk assessments, policies, guides and study documentation (such as data management plans, protocols).

Data security and protection practices (or Information governance) refers to the policies, procedures, processes, strategies, systems and controls implemented to manage information in an organisation so that the security and confidentiality of information is assured and so that the organisation abides by all appropriate regulatory and legal frameworks. There is no single standard definition but all definitions contain these ideas.

The Data Security and Protection (DSP) Toolkit is the successor framework to the Information Governance (IG) Toolkit. The DSP Toolkit is an online tool which allows health and social care organisations to measure their performance against the National Data Guardian's 10 data security standards.

Information assets are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation; they can include documents, staff and equipment.

An information risk strategy provides a structured and coherent approach to identifying, assessing and managing risk. It builds in a process for regularly updating and reviewing the assessment based on new developments or actions taken.

2. Purpose

The purpose of this Policy is to ensure all staff working within the Pragmatic Clinical Trials Unit (PCTU), and third parties as appropriate, understand their duties and responsibilities in relation to information governance and data security and protection by:

- providing a framework for robust information governance and data security and protection within the PCTU, in particular for preserving the confidentiality, integrity, security and accessibility of data, including compliance with appropriate regulatory and legal requirements relating to information governance
- clarifying the general principles under which staff and third parties work in relation to information governance and data security and protection
- providing a reference document to aid quality improvement
- outlining staff responsibilities

3. Scope

This policy applies to all information, information systems, computer networks, software applications, hardware and locations. It can sometimes be helpful to break this list down further

into definable information assets. All staff and other individuals listed here are also required to comply with all other relevant QMUL policies as appropriate [reference 3.1].

The policy applies to all staff employed or working on behalf of the PCTU, volunteers, and contractors. This includes PCTU staff with permanent and temporary contracts, those on placements and fellowships within the unit, contractors, parties external to the PCTU both within and outside Queen Mary who are working on PCTU linked projects and need to access data and information held by the PCTU, auditors and inspectors. It does not include visitors who are not carrying out any direct work or work on behalf of PCTU. Third party organisations providing services to the PCTU are also required to comply with this Policy and all other relevant QMUL Policies that apply to the type of services they provide.

4. Policy statement

4.1 Introduction

The PCTU undertakes to implement effective information governance practices to ensure the following:

- Information is protected against unauthorised access;
- Confidentiality of information is assured;
- Integrity of information is maintained;
- Information is supported by the highest quality data;
- Regulatory and legislative requirements are met;
- Data security and protection training is available to all staff as necessary to their role;
- All breaches of confidentiality and information security, actual or suspected, are reported and investigated.

There are six key interlinked strands to this Data Security and Protection Policy:

1. Openness
2. Legal compliance
3. Information security
4. Quality assurance
5. Internal accessibility of information
6. Risk

4.2 Openness

- Non-confidential information about the PCTU and its services is available to the public through a variety of media, in line with QMUL policies and any PCTU internal policies as laid out by senior management.
- PCTU abides by the QMUL Freedom of Information Policy [reference 4.2.1 & 4.2.2] to ensure compliance with the Freedom of Information Act 2000 [reference 4.2.3]

- PCTU follows QMUL's procedures and arrangements for liaison with the press and broadcasting media [reference 4.2.4]

4.3 Legal Compliance

- PCTU complies with the Data Protection Act 2018 and QMUL policy and procedure regarding data protection [reference 4.3.1 & 4.3.2 & 4.3.3] and responds appropriately to data subject to access requests within the timescales defined under the Act
- PCTU regards all identifiable information relating to study participants and staff as confidential except where exemptions can be applied. Access to information is always appropriately controlled. Staff have access to appropriate information regarding all relevant legislation and guidance relating to information security and confidentiality
- Direct consent will be sought from study participants where appropriate for the collection, processing and disclosure of data
- PCTU adheres and abides by all the applicable QMUL policies to ensure compliance with the common law duty of confidentiality and all relevant Acts of Parliament. [reference 4.3.4 & 4.3.2]
- Study participants and/or staff information is shared with other agencies in accordance with agreed protocols and relevant legislation. No participant data from research studies is shared with those outside the PCTU or those not directly involved in the research without an appropriate agreement being in place [reference 4.3.5], whether or not the data remain wholly within the defined safe haven and control of the PCTU.

4.4 Information Security

- PCTU in liaison with QMUL IT Services has authorisation procedures for the use and access to confidential information and records. [reference 4.4.1 & 4.4.2]
- PCTU, in line with QMUL Policies, has procedures for the effective and secure management of its information assets and resources [references 4.4.3 & 4.4.4 & 4.4.5 & 4.4.6 & 4.4.7]
- When they are not at their desks, PCTU staff keep desks free from hard copy or electronic devices containing accessible confidential or sensitive information including usernames, passwords, and restricted notes and minutes. PCTU promotes effective confidentiality and security practice to its staff through policies, procedures and training
- PCTU has incident reporting procedures which include the monitoring and investigation, where appropriate, of reported instances of actual or potential breaches of confidentiality and security. Where appropriate, PCTU abides by QMUL policies and procedures in relation to incident management and reporting [reference 4.4.8 & 4.4.9]
- PCTU follows QMUL guidelines on using mobile computing devices [reference 4.4.10]
- Further details on incident management can be found in our information security guidelines [4.4.5] and/or Central IT Services incident management procedures.

4.5 Information Quality Assurance

- PCTU has policies and procedures for information quality assurance and the effective management of records [reference 4.5.1 & 4.5.2]
- Wherever possible, information quality is assured at the point of collection in the first place and follows corresponding PCTU procedures on quality control and data validation [reference 4.5.3]

4.6 Internal accessibility to information

- All PCTU staff are provided with appropriate access to policies, SOPs and associated documents, induction and guidance documents, templates and forms, reports and meeting minutes to fulfil their roles
- Documents are stored with appropriate access arrangements in place depending on whether they are deemed (i) publicly accessible (ii) current and available to all staff, (iii) in draft, or (iv) restricted. Documents are stored on shared QMUL folders and/or Q-pulse as appropriate.
- Document access and storage arrangements are reviewed as and when necessary by the relevant responsible staff to ensure consistency and completeness.

4.7 Risk

- The PCTU will develop and operate an information risk strategy [4.7.1]

5. Staff responsibilities

5.1 Responsibilities of all staff

All new staff receive training regarding information governance and data security and protection in general and the following areas in particular. Further training is provided by the PCTU as appropriate. A questionnaire is undertaken each year to ascertain general understanding and followed by appropriate training at a staff meeting. Individual staff members are responsible for ensuring that they are up to date in the following areas

- Be aware of and familiar with this information governance policy – all staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it
- If employed by QMUL and employment contract was issued before February 2016, sign and abide by the PCTU's non-disclosure agreement [reference 5.1.1]
- Be proactive in ensuring they are adequately trained [5.1.2]
- Be aware of and abide by institutional and local guidelines on sharing confidential personal information [reference 5.1.3]

- Be aware of and familiar with institutional guidelines regarding auditing of confidentiality procedures [reference 5.1.4]
- Be aware of and familiar with institutional and local guidelines regarding secure transfer and receipt of personal and sensitive data [references 5.1.5 & 5.1.6]
- Be aware of, and use as necessary, institutional and local procedures for reporting IT security incidents [reference 4.4.9]

5.2. Specific responsibilities and accountabilities

The designated **Information Governance Lead** for PCTU is currently the PCTU Head of Information Systems and Data Management. The day to day responsibilities for providing guidance to staff within the unit will be undertaken by the PCTU Head of Information Systems and Data Management with support from the PCTU Caldicott guardian and Quality Assurance Manager. Information Asset Owners have specific responsibilities for information assets in particular areas within the PCTU. As the host institution for the PCTU, QMUL are responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct, the NHS information governance assurance framework and other relevant regulatory requirements.

The following table gives a very brief description of the main responsibilities of key individuals within the PCTU in relation to information governance.

Information governance title	**Assigned to (job title for individual)**	**Responsibility**
Senior information risk owner	Director	1. To ensure information assets and risks within the PCTU are managed as a business process rather than as a technical issue 2. To instil a culture within the PCTU to ensure that this happens 3. To establish an information risk strategy
Information governance lead	Head of Information Systems and Data Management; IG Lead	1. To oversee the development and implementation of IG procedures and processes ensuring quality improvement in the area of IG 2. To raise awareness and provide advice and guidance about IG to all staff ensuring that they are fully informed of their responsibilities 3. To ensure that any required staff training is completed 4. To coordinate the activities of any other staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities

		5. To ensure that personal data is kept secure and that all data flows, internal and external, are periodically checked against the Caldicott Principles 6. To coordinate, publicise and monitor appropriate standards of information handling throughout the PCTU ensuring compliance with law, guidance and internal procedures
Caldicott guardian	Head of Operations	1. To ensure protection of the confidentiality of study participant and employee information 2. To enable appropriate information-sharing
IG Assistant	IG Assistant	3. To assist the IG Lead on the development and implementation of IG within the unit, including training spot checks, documentation review and update, incident reporting 4. To actively support all activities related to the yearly DSPT assessment 5. To actively liaise with and support associated units/teams and ensure compliance with existing IG procedures To act as IAA for Information Governance and DSP 6.
Information asset owners 1. management /quality assurance 2. IT/data management 3. trial/study management 4. statistics 5. health economics	1. Head of Operations 2. Head of Information Systems and Data Management; IG Lead 3.Trial/study management team lead 4. Statistics team lead 5. Health economics team lead	1. To understand what information is held within the PCTU, what information is added and removed, how information is moved, and who has access and why 2. To understand and address risks to the information, and ensure that information is fully used within the law for the public good 3. To provide a written judgement of the security and use of their assets to support audits as necessary Each of the information asset owners is responsible for the assets within the area specified. Note that in each of these areas there may also be information asset administrators (IAAs) who assist the relevant information asset owner (IAOs). Their role is to ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

6. Communication, review and monitoring of this policy

- PCTU staff are made aware of this policy and the location of referenced documents at induction.

- This policy is reviewed annually by the PCTU IG committee and approved by the management group, and revised as necessary. Following review, all team leads are responsible for ensuring staff are aware of their responsibilities as set out in this policy
- Compliance with this policy is assured through:
  - Periodic audits undertaken or arranged by the PCTU of arrangements for openness and liaising with the public, compliance with legal requirements for internal document storage and access
  - Regular appropriate compliance questionnaires to all staff, spot checks and update training
  - Regular review of other relevant document
  - Updating all staff on legal requirements when necessary

7. References

If you have trouble locating what you think you need amongst these references please contact the PCTU Information Governance Lead for assistance.

Ref	File path	Owner	Details
Information governance			
[1.1]	DSP Toolkit ▪ About the DSP Toolkit ▪ Data Security Standards overall guide ▪ Assertions and evidence items	NHS digital	Information about the DSP Toolkit and the associated assertions and evidence items.
Relevant QMUL policies			
[3.1]	QMUL ARCS - Policy Zone	QMUL	QMUL policies; those most relevant to this policy will be in the *research, staff* and *IT* sections.
Openness			
[4.2.1]	QMUL - Freedom of information and publications scheme	QMUL	Freedom of information policy
[4.2.2]	JRMO – Freedom of Information SOP	QMUL	JRMO SOP for processing Freedom of Information Act requests
[4.2.3]	Legislation.gov.uk - Freedom of Information Act 2000	UK government	Freedom of Information Act 2000
[4.2.4]	QMUL - Media and Public Relations ▪ Media guide for staff: Working with the Public Relations team and journalists ▪ Information for journalists	QMUL	Guidance for liaising with press and broadcast media
Legal requirements			

[4.3.1]	Legislation.gov.uk – Data Protection Act 2018	UK government	Data Protection Act 2018
[4.3.2]	QMUL ARCS – Data Protection Policy Version 3.0	QMUL	Data protection policy
[4.3.3]	JRMO - Data Protection for research projects Version 5.0	QMUL	JRMO SOP on data protection
[4.3.4]	QMUL ARCS – Information Security Policies Version 6.1	QMUL	Information Security Policy to ensure compliance with relevant UK common law and legislation on confidentiality
[4.3.5]	PCTU Information Governance policies shared folder: ▪ Data Sharing SOP Version 1.0 PCTU Information Governance Guidance and Checklists shared folder: ▪ Data Sharing Guidance Version 1.0 PCTU Data Sharing Committee documents shared folder: ▪ Data Sharing Committee Terms of Reference Version 1.0	PCTU	Information about the PCTU's data sharing processes via the Data Sharing Committee.
Information security			

[4.4.1]	PCTU Trial Management SOPs folder Trial Management sub-folder: ▪ Document Completion Transport and Storage Version 4.0 ▪ Site Initiation Version 4.0 ▪ Handling Trial Correspondence Version 4.0 Trial Closure sub-folder: ▪ Archiving Research Projects SOP Version 4.0 QMUL - Third Party Access to Information Policy Version 2.0	PCTU QMUL	QMUL and PCTU SOPs of particular relevance for accessing confidential information
[4.4.2]	QMUL ITS - System Access Controls SOP Version 1	QMUL	System Access Controls SOP
[4.4.3]	QMUL ITS - Password Management Policy Version 2.1	QMUL	Password Management policy
[4.4.4]	QMUL ITS - User Account Management Policy Version 2.3	QMUL	User Account Management Policy
[4.4.5]	PCTU Information Governance Guidance and Checklists shared folder: ▪ PCTU Information Security Guidelines – latest version	PCTU	Information security guidelines
[4.4.7]	QMUL ITS - Handling Information SOP Version 1.2	QMUL	Handling Information SOP
[4.4.8]	QMUL ITS - Security Incident Management SOP Version 1	QMUL	Security Incident Management
[4.4.9]	QMUL ITS - Information Security Incident Reporting policy Version 2.0	QMUL	Information Security Incident Reporting
Information quality assurance			
[4.5.1]	QMUL ITS - Records Management SOP Version 1.0	QMUL	Records Management SOP
[4.5.2]	PCTU Data Management SOPs shared folder:	PCTU	SOPs of particular relevance to quality control of data

	▪ Data Entry Quality Control Data Extraction and Database Lock SOP Version 3.0 ▪ Data Security SOP Version 2.0		
[4.5.3]	PCTU Data Management SOPs shared folder: ▪ Data Entry Quality Control Data Extraction and Database Lock SOP Version 3.0	PCTU	Data Entry, Quality Control, Data Extraction and Database Lock SOP
Risk			
[4.7.1]	PCTU Business and Admin Guidance and Checklists shared folder: ▪ Risk Management Strategy Version 1.0	PCTU	Risk management strategy
Staff responsibilities			
[5.1.1]	PCTU Information Governance templates shared folder: ▪ Non-disclosure agreement Version 2.0	PCTU	Non-Disclosure-Agreement v2.0
[5.1.2]	https://ess.q-review.qmul.ac.uk/ess/echo/presentation/fcff1e4d-103e-4ddf-a9f6-270a034d9cfd https://ess.q-review.qmul.ac.uk/ess/echo/presentation/9365512b-7a95-46ec-b160-87780f52648d https://ess.q-review.qmul.ac.uk/ess/echo/presentation/ddd4a053-8324-4c90-aa8c-abc6202a10e9	NHSD	Links to part of PCTU interim training materials (Added March 2017: Please note that additional training materials may be made available and training requirements updated during this interim period, until new NHSD online training resources are back online).
[5.1.3]	QMUL ARCS – Research Data Access and Management Policy	QMUL	Research Data Access and Management Policy
[5.1.4]	JRMO – Data Protection for Research Projects SOP	QMUL/ JRMO	QMUL information on auditing of confidentiality procedures

[5.1.5]	PCTU Data Management SOPs shared folder: ▪ Data Transfer SOP Version 3.0	PCTU	Data Transfer SOP PCTU_SOP_DM_11 Data transfer v 3.0

Document Control

Version	Reason for Change	Author of change	Date
1.0	n/a	Arouna Woukeu	31.03.2015
2.0	General periodical review and update as specified within the policy	Arouna Woukeu	11.03.2016
3.0	Links to the references in section 7 were updated. Wording re non-disclosure policy was updated. Other minor wording updated. Information security guidelines attached as appendix in V 2.0 has been removed and authorised as a separate document.	Sandra Eldridge, Arouna Woukeu, Sally Kerry, Anita Patel, Anitha Manivannan, Natasha Stevens, Julie Dodds, Domenico Giacco.	22.03.2017
3.1	Update to electronic links and following comments at information governance meeting October 2017	Lisa Cammell, Sandra Eldridge	05/02/2018
3.2	Further updates to section 2	Sandra Eldridge	05/02/2018
3.3	Further updates after comments on 3.2	Sandra Eldridge, Arouna Woukeu, Lisa Cammell, Julie Dodds, Tash Stevens	08/02/2018
3.4	Further updates to finalise	Sandra Eldridge, Lisa Cammell, Tahera Hussain	09/02/2018
3.5	Removing all track changes	Sandra Eldridge	09/02/2018
3.6	Removing comments and changing “trial” to “study” where appropriate (note that some comments on version 3.5 need to be carried forward to next update).	Sandra Eldridge	27/02/2018
3.7	Minor admin changes and authorisation dates amended, All tracked changes removed	Anitha Manivannan, Sandra Eldridge	01/03/2018
4.1	Updates to wording relating to implementation of DSPT / replacement of IGTK and new guidance Reference links updated and hyperlinks added, formatted Updated names for new members of staff	Sarah Thomas	5/12/2018
4.2	Changed name of document back to IG Policy and a few minor changes to text	Ann Thomson	20/12/2018
4.3	A few minor changes	Sandra Eldridge	21/12/2018
4.4	Moved details of staff to whom policy applies from section 2 (purpose) to section 3	Sally Kerry	2/1/2019

	(scope) Changes to Data Sharing references. Minor comment changes to text		
4.5	Final review and update prior to approval Title changed to DSP Policy (previously IG Policy)	Arouna Woukeu	28/03/2019

Appendix A: Current roles and responsibilities

Information governance title	Assigned to (job title for individual)	Current individual	Information asset assistants (if applicable)
Senior information risk owner	Director	Sandra Eldridge	n/a
Information Governance lead	Head of Information Systems and Data Management	Arouna Woukeu	n/a
Caldicott guardian	Head of Operations	Tahera Hussain	n/a
Information Governance Assistant	IG Assistant	Sarah Elaine Thomas	n/a
Information asset owner (management/ quality assurance)	Head of Operations	Tahera Hussain	Charlotte Ayton-George Anitha Manivannan
Information asset owner (IT/data management)	Head of Information Systems and Data Management	Arouna Woukeu	Kalia Michael Sarah Elaine Thomas (IG & DSPT)
Information asset owner (trial/study management)	Projects and strategy lead	Ann Thomson	Maria D'Amico
Information asset owner (statistics)	Reader in medical statistics	Sally Kerry	Chris Newby
Information asset owner (health economics)	Chair in health economics	Boby Mihaylova	Chris Roukas
Assistant Information Governance lead at the Unit for Social and Community Psychiatry	Research Fellow	Domenico Giacco	Carolanne Ellis-Brewer
Assistant Information Governance Lead for Centre for Primary Care and Public Health - Women's Health Research Unit	Senior Research Manager	Julie Dodds	n/a
Assistant Information Governance Lead in the National Bowel Research Centre	Senior Trials Manager	Shiva Taheri (interim)	n/a

Assistant Information Governance Lead for Centre for Primary Care and Public Health (excluding Women's health)	Clinical Trial Monitor	Jeanette Hansen	n/a
Assistant Information Governance Lead for Critical Care and Perioperative Medicine Research Group	Senior Trials Coordinator	Priya Dias	n/a
Assistant Senior Risk Information Owner at the Unit for Social and Community Psychiatry	Professor of Social and Community Psychiatry	Stefan Priebe	n/a
Associate Senior Risk Information Owner Primary Care and Public Health - Women's Health Research Unit	Professor in Maternal and Perinatal Health	Shakila Thangaratinam	n/a
Associate Senior Risk Information Owner at the National Centre for Bowel Research	Clinical Professor of Surgical Research,	Charles Knowles	n/a
Associate Senior Risk Information Owner at Primary Care and Public Health (excluding Women's health)	Professor in Public Health and Primary Care	Stephanie Taylor	n/a
Associate Senior Risk Information Owner at Critical Care and Perioperative Medicine Research Group	Professor & Consultant in Intensive Care Medicine	Rupert Pearse	n/a