Barts and The London
School of Medicine and Dentistry

PCTU

Information Governance Policy

Pragmatic Clinical Trials Unit (PCTU)

Policy number	PCTU_POL_IG_01	Version number	4.0
Publication date	9 March 2018	Review date	9 March 2019

Author:	Arouna Woukeu
Reviewed by:	Sandra Eldridge

Authorisation:	
Name / Position	Arouna Woukeu - PCTU Information Governance Lead
Signature	AW
Date	9 March 2018

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.

Information governance provides a way for employees to deal consistently with the many different rules about how information is handled such as The Data Protection Act, The common law duty of confidentiality, The Freedom of Information Act etc.

NHS digital is commissioned by the Department of Health to develop and maintain rules, policies and guidance regarding information governance that all Health and Social Care service providers, commissioners and suppliers need to comply with. These rules, policies and guidance are drawn together and grouped into categories in the Information Governance Toolkit, a set of information governance requirements. All organisations that have access to NHS patient data must provide assurances that they are practising good information governance and use the Information Governance Toolkit to evidence this.

The Pragmatic Clinical Trials Unit uses the framework of the Information Governance Toolkit [references 1.1 & 1.2] to ensure a process of continuous quality improvement in relation to information governance within the unit.

Definitions

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

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 Information Governance Toolkit is a self-assessment exercise in which an organisation checks its information governance against the relevant standard. Organisations are required to meet different standards dependent on the type of organisation and the type of data they hold or have access to. The Toolkit describes the work toward complying with relevant requirements and maintaining the compliance.

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 (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) as appropriate, understand their duties and responsibilities in relation to information governance by:

- providing a framework for robust information governance 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
- 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, locations, and staff employed or working on behalf of the PCTU, including temporary staff, volunteers, and contractors. 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].

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 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;
- Information governance 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 Information Governance Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance
- Internal accessibility of information
- 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 1998 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 4.3.6], 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. IT related incidents are reported as per IT services procedures. Physical security incidents are reported to the appropriate Centre Manager who reports onwards as necessary. All other IG and data security incidents are primarily reported to the IG Lead, and by sending an email to the incident reporting mailbox, pctu-ig-incidents@qmul.ac.uk.
- Depending on incidents, study teams should also report appropriately to sponsors and other bodies as required.
- 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]

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 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 and the NHS information governance assurance framework.

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	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 training made available is taken up 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

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 3.Trial management team lead or designated Senior Trial Manager 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 leaders 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]	https://www.igt.hscic.gov.uk/RequirementsList.aspx?tk=421404816360094&lnv=2&cb=fca393af-cc40-407b-839e-bc1cc741baf7&sViewOrgType=22&sDesc=Hosted%20Secondary%20Use%20Team/Project	NHS digital	Information Governance Toolkit Requirements
[1.2]	https://www.igt.hscic.gov.uk/Home.aspx?tk=421404816360094&cb=32665528-c03a-4b93-a85c-10bee21521ac&lnv=7&clnav=YES	NHS digital	General information about the Information Governance Toolkit and reports from all participating organisations
Relevant QMUL policies			
[3.1]	http://www.arcs.qmul.ac.uk/policy/index.html	QMUL	QMUL policies; those most relevant to this policy will be in the *research, staff* and *IT* sections.
Openness			
[4.2.1]	http://www.qmul.ac.uk/about/collegeinfo/index.html	QMUL	Freedom of information policy
[4.2.2]	http://www.jrmo.org.uk/media/jrmo/docs/performing-research/sops/SOP_32_FOI_v5.0_WEBSITE.PDF	QMUL	JRMO SOP on Freedom of information act request
[4.2.3]	http://www.legislation.gov.uk/ukpga/2000/36/contents	UK government	Freedom of Information Act 2000
[4.2.4]	http://qm-web.mc.qmul.ac.uk/publicrelations/Media%20training/index.html	QMUL	Guidance for liaising with press and broadcast media
Legal requirements			
[4.3.1]	http://www.legislation.gov.uk/ukpga/1998/29/contents	UK government	Data Protection Act
[4.3.2]	http://www.arcs.qmul.ac.uk/media/arcs/policyzone/Data-Protection-Policy-2009-v02.3.pdf	QMUL	Data protection policy
[4.3.3]	http://www.jrmo.org.uk/media/jrmo/docs/performing-research/sops/medical-sops-2/SOP-16-Data-Protection-for-research-projects-v5-0-reissued.pdf	QMUL	JRMO SOP on data protection
[4.3.4]	http://www.arcs.qmul.ac.uk/media/arcs/policyzone/IS-Policies-v06.1.pdf	QMUL	Information Security Policy to ensure compliance with relevant UK common law and legislation on confidentiality
[4.3.5]	J:\PCTU_AllStaff\PCTU-Policies\POL_IG / PCTU_POL_IG_02_Data Sharing Policy_v3.0 J:\PCTU-All-Staff\Guidance & Checklists\IG\Current I.G. Guidance	PCTU	PCTU_POL_IG_02_Data sharing policy v 3.0

	and Checklist/ PCTU_GUI_IG_04_Data Sharing Guidelines_v1.0 J:\PCTU-All-Staff\Templates\IG\Current I.G. templates\TEM_IG-01 Data Sharing template/ PCTU_TEM_IG_01 Data sharing template V 2.0_final_signed J:\PCTU-All-Staff\Templates\IG\Current I.G. templates\TEM_IG_02 Data Access Request Form J:\PCTU_Admin\PCTU Data Sharing Committee\Documents\Terms of Reference/ PCTU_Data sharing committee terms of reference v 1.0 - signed		PCTU_GUI_IG_04 Data Sharing Guidelines V 1.0 PCTU_TEM_IG_01 Data sharing template V2.0 PCTU_TEM_IG_02 Data Access Request template v 1.0 PCTU_Data sharing committee terms of reference v 1.0 – signed
Information security			
[4.4.1]	J J:\PCTU-All-Staff\SOPs\Current\Trial Management\Trial Management	PCTU	SOPs: of particular relevance to access to confidential information SOPs: PCTU SOP TM_07 Document Completion Transport and Storage v3 PCTU SOP TM_09 Site Initiation v3 PCTU SOP TM_10 Handling Trial Correspondence v3
	J:\PCTU_AllStaff\SOP_ COMPLETE\Trial Closure	PCTU	PCTU SOP TC_02 Archiving Research Projects v3
	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142313.pdf	QMUL	QMUL SOP DG03 Confidentiality Agreements
[4.4.2]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142321.pdf	QMUL	SOPs on system access controls

[4.4.3]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142328.pdf	QMUL	password management policy
[4.4.4]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142327.pdf	QMUL	IT User Account Management Policy
[4.4.5]	J:\PCTU_AllStaff\Guidelines and Checklists\IG	PCTU	Information security guidelines
[4.4.6]	J:\PCTU-All-Staff\Guidance & Checklists\IG\Current I.G. Guidance and Checklist/PCTU_GUI_IG_07_Information security guidelines_v2.0	PCTU	PCTU_GUI_IG_07_Information Security Guidelines_v1.0
[4.4.7]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142325.pdf	QMUL	Handling Information SOP
[4.4.8]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142338.pdf	QMUL	ITS Security Incident Management
[4.4.9]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142315.pdf http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142315.pdf	QMUL	Information Security Incident Reporting & IT Security Incident Management.
Information quality assurance			
[4.5.1]	http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142323.pdf	QMUL	Records Management
[4.5.2]	J:\PCTU-All-Staff\SOPs\Current\DM	PCTU	SOPs: of particular relevance to quality control of data are SOPs: PCTU_SOP_DM 04_Data Entry Quality Control Data Extraction and Database Lock V 2.0 PCTU_SOP_DM_05 Electonic Data Security v1.0
[4.5.3]	J:\PCTU-All-Staff\SOPs\Current\DM\PCTU_SOP_DM 04_Data Entry Quality Control Data Extraction and Database Lock V 2.0	PCTU	PCTU_SOP_DM 04_Data Entry Quality Control Data Extraction and Database Lock V 2.0
Risk			
[4.7.1]	J:\PCTU-All-Staff\Guidance & Checklists\Business-Admin\Current Guidance and Checklist documents\PCTU_GUI_BU_17_PCTU Risk management strategy_v1.0	PCTU	Risk management strategy
Staff responsibilities			
[5.1.1]	J:\PCTU-All-Staff\Templates\IG	PCTU	Non-Disclosure-Agreement v2.0
[5.1.2]	https://ess.q-review.qmul.ac.uk/ess/echo/presentatio	NHSD	Links to part of PCTU interim training materials

	n/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		(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]	http://www.qmul.ac.uk/media/arcs/policyzone/Research_Data_Management_policy_for_publication_Dec13.pdf	QMUL	Research Data Access and Management Policy
[5.1.4]	http://www.jrmo.org.uk/media/jrmo/docs/performing-research/sops/medical-sops-2/SOP-16-Data-Protection-for-research-projects-v5-0-reissued.pdf	QMUL/ JRMO	QMUL information on auditing of confidentiality procedures JRMO SOP 16 Data Protection for Research Projects v.5.0
[5.1.5]	J:\PCTU-All-Staff\SOPs\Current\DM\PCTU_SOP_DM_11 Data transfer v 2.0	PCTU	PCTU_SOP_DM_11 Data transfer v 2.0

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
4.0	Update to electronic links and following comments at information governance meeting October 2017. Further updates to section 2. Further updates after comments on 3.2. Further updates to finalise. 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).	Lisa Cammell, Sandra Eldridge, Arouna Woukeu, Lisa Cammell, Julie Dodds, Natasha Stevens, Tahera Hussain, Anitha Manivannan	09/03/2018

	Minor admin changes and authorisation dates amended, All tracked changes removed.		

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 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 More TBC
Information asset owner (trial/study management)	Projects and strategy lead	Ann Thomson	TBC
Information asset owner (statistics)	Reader in medical statistics	Sally Kerry	Chris Newby Gordon Forbes
Information asset owner (health economics)	Chair in health economics	Boby Mihaylova	TBC
Assistant Senior Risk Information Owner at the Unit for Social and Community Psychiatry	Professor of Social and Community Psychiatry	Stefan Priebe	n/a
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 Research Nurse	Eleanor McAlees	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
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

Appendix B: Unit for Social and Community Psychiatry, Queen Mary University of London (USCP) - Internal Information Security Policy

Document History
Date 22/02/2017
Version 0.2 (Active)
Authors: Carolanne Ellis-Brewer, Domenico Giacco

Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support all operations and guarantee continued success. Physically secured hard files and security of soft files is essential.

With this in view, USCP recognises that adherence and compliance to the objectives set out in the Pragmatic Clinical Trials Unit (PCTU) Information Governance Policy (IG Policy) is a fundamental requirement. This Internal Information Security Policy is supplementary to the PCTU IG Policy and outlines the practical implementation of the Policy's objectives regarding internal security at the USCP. It aims to ensure and maintain the confidentiality, integrity and availability of PCTU information stored, processed and communicated by and within the USCP. It deals with the implementation of several measures, checks and procedures that collectively guarantee the integrity and confidentiality of information, networks and devices such as PCs, laptops, removable storage etc. and that documents, offices and other assets are protected from unauthorised access.

Particular responsibilities within this guide are defined as:-

Review and maintenance: Carolanne Ellis-Brewer and Domenico Giacco
Approval: Stefan Priebe
Monitoring: Carolanne Ellis-Brewer and Domenico Giacco
Local adoption: Stefan Priebe, Carolanne Ellis-Brewer and Domenico Giacco

Staff and visitor access security

USCP staff will be given a full induction and access credentials (photo ID swipe card/pin number) to gain access to secured areas of the Newham site.

1) Access for USCP staff, whether from East London NHS Foundation Trust (ELFT) or Queen Mary University of London (QMUL), is gained through the side of the building using swipe access.

2) Non-USCP visitors enter the building though the side entrance by pressing the buzzer (manned between 9:00 and 17:00) and announcing who they are. They are requested to come to the top of the stairs where an administrator will meet them. They are then required to sign the visitor'' book and will be issued a visitor pass for the duration of their stay. Staff will be asked to collect and escort non-USCP visitors.

3) Access to secure areas by maintenance personnel will be allowed as required.

These procedures will be reviewed at intervals of not more than one year.

In the event of any serious incident or change affecting these procedures, a recommendation will be made and new procedure incorporated.

Clear Desk and Screen Policy

Due to the confidential nature of work, the ELFT and the USCP encourage a "Clear Desk" policy. ('Clear Desk' in the IG context is meant for 'clear' from confidential information as itemised below):

1) Desks should be free from documents or electronic devices with any confidential information such as usernames, password, notes or minutes etc. or other related information that might directly or indirectly compromise security. Usernames and password should NOT be written down in any way that could be discovered and to do so causes a breach of the Information Governance Policy.

2) If hard-copy confidential information is no longer required, it should be destroyed as soon as possible. Ensure documents are shredded using the in-house shredding machine.

3) All staff must either lock or log off their computer when they leave their desks and also at the end of the day or when leaving the office, to prevent unauthorised access to systems and confidential information.

4) Screensaver passwords are set to activate after a specified period of inactivity to ensure no unauthorised access to our systems.

5) It is a shared duty and responsibility that all offices, whether single or open, are not left unlocked and unoccupied. All offices within the USCP are locked by security staff at the end of the day, or when the last employee has left.

Control Procedures for Laptops

The USCP has responsibility for the control of laptops, computers or other mobile computing devices issued by the ELFT or QMUL and that are used for accessing systems and data in the USCP. Only these devices may be used for accessing clinical research study data and associated information. The ELFT and QMUL issue such devices that have up-to-date security vulnerability fixes, anti-virus applications and approved and secure versions of applications used for access. Additionally, in the event of data being compromised or lost, a log (**the Information Assets Register**) of devices (laptops, etc.) is kept and can be used to trace any problems.

Laptops are restricted for use by staff within the USCP. To gain access to a laptop the employee must have a relevant user name and password. Laptops should not be used to store confidential information as laptops may be shared.

When using such a laptop and if away from the desk for any length of time, the laptop must have the network account locked and the laptop itself secured.

Employees who use laptops at other sites should always be aware of unauthorised parties who may be "shoulder surfing" (watching what is being typed and/or displayed information), which poses a security risk.

Employees are responsible for their assigned laptops; at the end of each day they should secured and, if being left at work, placed in a lockable drawer or cabinet.

Consideration must be given when transporting a laptop. It is advisable to place the laptop in the boot of a car whilst in transit, if at all possible. Laptops and any electronic devices should not be left unattended in any form of travel or while on visits at other sites.

For laptops belonging to the USCP, the network connections and user accounts, data being accessed using them and information (emails, documents etc.) held in them, create potential risks for unauthorised access to USCP/PCTU data and information. These guidelines intend to minimise this risk.

Software and applications

Under no circumstances must unauthorised firmware or software be used or downloaded onto laptops. All PCs used within the USCP are already protected by IT regulations on unauthorised downloading of software. All staff at the Unit for Social and Community Psychiatry migrated to nhs.net email addresses, which are deemed as a secure service and authorised for sending sensitive information, such as clinical data, between NHSmail and: a) other NHSmail addresses (i.e. from an '*.nhs.net' or '.hscic.gov.uk' account to an '*.nhs.net' or '.hscic.gov.uk' account); b) other email systems that comply with the SCCI 1596 secure email standard; c) other email systems that comply with the pan-government secure email standard (please see: https://portal.nhs.net/Home/AcceptablePolicy)

Data Security procedure

Access to the Trust's I:/drive system: all USCP (Trust and QM) employees who work at the Newham site on a regular basis have access to the shared I:/drive which is ring-fenced for the USCP. However, all datasets are security protected and all access to data is subject to

authorisation by the Head of the USCP (Stefan Priebe). No visitors are allowed access to the I:/drive without specific authorisation by the Head of the USCP (Stefan Priebe).
When patient identifiable data need to be stored (e.g. in order for research participants to be followed up), electronic files are stored in protected folders as set up by IT at ELFT and paper documents are in locked cupboards. Patient identifiable data are accessed on a need to know basis only by the staff working on the specific project for which storing identifiable data is required.

Remote communication will be through a secured authentication outlined by QMUL IT Services 'Remote Access Policy V1.5, updated 22/10/2015'[1]. Data access levels will be strictly controlled and permission to access will be granted by the USCP Manager (Carolanne Ellis-Brewer), with approval from the Head of the USCP (Stefan Priebe).

Physical Security Procedure

The premises of the USCP are considered a secure location with the following procedures in place:

- Swipe card access.
- Conventional lock for out of hours.
- All doors into the Unit are locked once staff have left the building. This includes all office doors, the doors into the main research office and cupboard and storage locks.

Security Controls - External

The outside door to the side of the building is accessed by swipe card for employees.
Visitors must buzz to gain entrance.

Any breach in this procedure should be reported immediately and treated as a security incident, so that countermeasures can be put in place immediately.

Any defects, such as doors not being secure or held open by any means, should also be reported.

Security controls - Internal

Any breach in this procedure should be reported immediately and treated as a security incident, so that countermeasures can be put immediately in place.

Any defects, such as a window not closing, should also be reported immediately.

b.1) Equipment

No USCP equipment is accessible for non-USCP visitors.

[1] http://www.its.qmul.ac.uk/Documents/Governance/SOPs/142329.pdf

Removal of equipment from the USCP is only permitted with written permission from the Head of the USCP (Stefan Priebe) and this should be done in accordance with the Asset Management and Control procedure.

The locked cupboards in which paper data and employee information are stored are described in detail in the “Asset register”.

Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this policy.

Review and Monitoring

The USCP has in place routines to regularly audit compliance with this and other policies. There is an Asset Register that records all physical assets for the Unit.