PHI | Public Health Institute
LIVERPOOL JOHN MOORES UNIVERSITY

DPA02

Confidentiality Code of Conduct

For all staff at

PUBLIC HEALTH INSTITUTE,
LIVERPOOL JOHN MOORES UNIVERSITY

Document Reference:	DPA02
Author:	Geoff Webb
Version.Issue:	1.1
Status:	Approved
Approved by:	Dave Seddon
Version date:	November 2017
Review date:	November 2018

Approval and Authorisation

Completion of the following detail signifies the review and approval of this document, as minuted in the senior management group meeting(s) shown.

Version	Authorising Group	Name of Approver	date
1.0	DPA Compliance Group	Dave Seddon	22/10/13
1.0	DPA Compliance Group	Dave Seddon	30/10/14
1.0	DPA Compliance Group	Dave Seddon	05/11/15
1.1	DPA Compliance Group	Dave Seddon	10/11/16
1.1	DPA Compliance Group	Dave Seddon	06/11/17

Document change history

Version	Status	Reason for change	date	Author
0.1	Draft	First draft version	20/05/2013	Geoff Webb
0.2	Draft	Change logo size & position	20/05/2013	Geoff Webb
1.1	Full	Changed CPH to PHI	05/11/2016	Mark Whitfield

Contents

1. Introduction

PHI's documented and implemented processes and procedures provide a consistent approach in the provision of research, data monitoring and analysis, which take into account the guidance, recommendations and obligations of the following:

- Caldicott - care in confidentiality of patient identifiable information
- Informed consent to disclosure of patient identifiable information
- Information Quality Assurance
- Information Security Management recommendations of ISO/IEC 27001:2005
- Common law duty of confidentiality
- Data Protection Act 1998
- Records Management – including Health Records
- Freedom of Information Act 2000

Effective processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality. Where there are weaknesses in an organisation's information governance, its controls on access to confidential data are unlikely to be effective and it would not therefore be possible to comply with required levels of information governance management, confidentiality and data protection assurance and information security assurance.

PHI is committed to ensuring that the confidentiality of those who give information, and those who are the subject of information, is respected and that their rights in relation to identifiable information are protected.

PHI is committed to enabling those working with information to have an effective understanding of their obligations regarding confidentiality.

1.1 Purpose

The principle behind this Code of Conduct is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the PHI's security systems or controls in order to do so.

Non-compliance with this Code of Conduct by any person working for PHI may result in disciplinary action being taken in accordance with PHI's disciplinary procedure, which could include dismissal or termination of contracts.

This document is a statement of required practice for those who work within or under contract to PHI concerning confidentiality of staff and patient information and patients' consent to the use of their health records. Its key reference is the Department of Health guidance *"Confidentiality: NHS Code of Practice" -November 2003.*

2. Definitions

The following are definitions of words or phrases used within this Confidentiality Code of Conduct and which have specific meanings:

- **Staff**
  - all directly employed staff, all locums, students, trainees, secondees, staff on temporary placements working under PHI management, and all contractors, agency staff or consultants under the direct management of PHI or carrying out work commissioned by PHI.

- **Relevant filing system**
  - any set of information relating to individuals which is structured whether by reference to individuals or criteria relating to individuals, in a way that specific information relating to an individual is readily accessible.

- **Data Controller**
  - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed e.g. NHS Organisation.

- **Processing**
  - wide definition including obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, aligning, storing, combining, blocking, erasing or the destruction of the information or data.

- **Data Subject**
  - an individual who is the subject of the personal data.

- **Authorised User**
  - a person who has been officially issued with a password for access to a particular system to carry out legitimate duties.

- **Subject Access Request**
  - application by, or on behalf of, the data subject under the Data Protection Act 1998 for access to information held about them.

- **Health Professional**
  - definition includes registered medical practitioners, dentists, opticians, pharmaceutical chemists, nurses, midwives, health visitors, osteopaths, chiropractors, clinical psychologists, child psychotherapists and speech therapists .

- **Access to patient identifiable data:**
  - In order to minimise the risk of breaches of legislation and mandatory codes of practice, the default access for all individuals to whom this policy applies will be as follows:
    - No access to patient identifiable data unless otherwise approved by the Data Guardian within the terms of this policy and any other applicable Organisation policies governing access to data.

- **Person Identifiable Data (PID)**
  - This term applies to **a combination of some of** the following data items wherever it/they may appear and irrespective of the name of any data field in which it/they may appear, allowing that patient to be identified:

        - Name - including last name and any forename or aliases
        - Address – including any current or past address of residence
        - Postcode - including any current or past postcode of residence
        - Date of birth
        - NHS number
        - Ethnic category
        - Local Patient identifier
        - Hospital Encounter number
        - Patient pathway identifier
        - SUS spell ID
        - Unique booking reference number
        - Date of death

- **Data Locations**
    - This term applies to data stored on hardware and equipment directly managed, owned or hired by PHI including but not limited to:

        - Servers on Organisation premises
        - Servers on non- Organisation premises
        - Desktop computers on Organisation premises
        - Desktop computers on non- Organisation premises
        - Laptops, notebooks and netbooks
        - PDAs, mobile phones
        - Memory cards and memory sticks

- **Data Formats**
    - This term applies to data stored in the following formats including but not limited to:
        - Oracle (or equivalent)/Business Objects data repositories
        - SQL Server (or equivalent) data repositories
        - Microsoft Access (or equivalent) databases
        - Microsoft Excel (or equivalent) spreadsheets
        - Microsoft Word (or equivalent) documents
        - Microsoft PowerPoint (or equivalent) presentations
        - Microsoft Publisher (or equivalent)
        - Microsoft Sharepoint (or equivalent)
        - Plain text files in any format
        - Zip files (or equivalent)
        - PDF files
        - Emails and their attachments
        - Graphics files in any format
        - Other proprietary systems and their dedicated formats used to store or manipulate data

- **Pseudonymisation:**
    - As part of the NHS Information Governance Toolkit, a national project called the Pseudonymisation Implementation Project (PIP) was set up to oversee and support local PIP work required to achieve this compliance. It ensures that patient data is de-identified when used for secondary use purposes.

3. Roles and Responsibilities

3.1 Data Guardian

The PHI Data Guardian has a particular responsibility for reflecting staff and patients' interests regarding the use of identifiable information and is responsible for ensuring such information is stored, used and shared in an appropriate and secure manner, in accordance with the rights of individuals.

In cases where staff are unsure of any aspect of confidentiality or for any advice on confidentiality, they should contact the Data Guardian.

3.2 All Staff

Each employed, contracted and voluntary staff member and authorised external user is personally responsible for ensuring that no breaches of computer security or information confidentiality result from their actions and must sign this agreement to signify compliance with PHI's relevant security and confidentiality policies and procedures.

4. Confidentiality

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

That confidentiality is:

- is a legal obligation that is derived from case law
- is a requirement established within professional codes of conduct; and
- must be included within PHI employment contracts as a specific requirement linked to disciplinary procedures

Information should be considered confidential if it can be related in any way to a specific individual. The main areas of concern are about patient and staff records and include any information that has not been fully anonymised. For example an NHS number, even in the absence of other personal information is not considered anonymous because it is still possible to trace that individual from the NHS number.

Confidential information will be found in a variety of formats including paper, computerised (including portable devices such as laptops and palmtops), visual and other versions of information storage media such as digital images and photographs. In addition, it covers oral communications including the use of the telephone (including mobiles) and general conversation.

5. Following the rules

5.1 Social Networking

All staff must be aware of the potential business risks and impacts associated with the use of blogging and social networking websites.

Where appropriate technical controls prevent access to such sites in the workplace, If there is a genuine need for access, staff must contact the IT Support Manager.

However, blogging and social networking websites are accessible out of the workplace so it must be recognised that it is easy to unwittingly give information while registering on a website that could be harmful to PHI or LJMU, for example if you disclose your profession and where you work.

Therefore when registering with a website, for your own personal security understand what you are signing up to and importantly what security and confidentially claims and undertakings exist.

Withhold personal details that you do not want to be made public.

You must not put work related information onto blogging or social networking sites.

It is important that all staff appreciate the need for responsibility and accountability in relation to the security and confidentiality of PID.

All staff must adhere to this policy and be aware that failure to do so could result in disciplinary action including dismissal.

5.2 Responsibilities

All staff have a responsibility to comply with the statutory acts that affect the processing and handling of information, confidentiality, the use of systems, and the protection of software.

These include:

- The Data Protection Act
- Freedom of Information Act
- The Computer Misuse Act
- The Copyright, Design and Patents Act
- The Human Rights Act
- Health & Social Care Act – Section 60
- The Access to Health Records Act 1990 (in the case of records for deceased patients)

5.3 Compliance

Staff must be aware of the need for compliance with the requirements of the Data Protection Act 1998 and all other associated legislation and guidance dealing with confidentiality and security. Full details of PHI's policies are on the intranet page at http://www.PHI.org.uk/governance

5.4 Good Practice

Good practice working should be applied in all areas including in the office, at a reception desk, in a laboratory or anywhere that information is moving into, out of and around PHI.

5.5 Data Protection 1998

The Data Protection Act 1998 is the fundamental legal requirement that applies to all organisations and individuals processing data of a personal nature. It is founded on the following set of eight principles:

- **Principle 1** – Personal data shall be processed fairly and lawfully and in particular shall not be processed unless specified conditions can be met.
- **Principle 2** – Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
- **Principle 3** – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Principle 4** – Personal data shall be accurate and where necessary kept up to date.
- **Principle 5** – Personal data processed for any purpose or purposes shall not be kept any longer than is necessary for that purpose or those purposes.
- **Principle 6** – Personal data shall be processed in accordance with the rights of data subjects.
- **Principle 7** – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
- **Principle 8** – Personal data shall not be transferred to any country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.6 Caldicott Report 1997

Following a review of confidential patient information by the NHS and the subsequent Caldicott report published in 1997, a series of recommendations for improvements to practice were made along with a basic set of six principles for all NHS organisations to adopt. The Caldicott Principles are currently under review and any changes will be reflected here.

- **Principle 1 – Justify the purpose**
  Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appointed Guardian.

- **Principle 2 – Only use it when absolutely necessary**
  Patient-identifiable information items must not be used unless there is no alternative.

- **Principle 3** – **Use the minimum necessary patient-identifiable information**
  Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

- **Principle 4 – Access to patient-identifiable information should be on a strict need to know basis**
  Only those individuals who need access to patient- information should have access to it and they should only have access to the information items that they need to see.

- **Principle 5 – Everyone should be aware of their responsibilities**
  Action must be taken to ensure that those handling patient identifiable information are aware of their responsibilities and obligations to respect patient confidentiality.

- **Principle 6 – Understand and comply with the law**
  Every use of the patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that PHI complies with legal requirements.

6. Acceptable Use for Email and Internet

6.1 General Principles

This document does not replace the Liverpool (John Moores) University Computing Facilities - conditions of use and associated policies which all staff must comply with.

This internet and e-mail Acceptable Use Guidance applies to all PHI employees, as well as people who are not directly employed but who use PHI equipment, IT facilities or data.

Although many employers are reasonable about the use of IT in the workplace for personal reasons, there is a growing awareness of how its misuse may be highly detrimental to the employing organisation, and monitoring or even outright bans are not now uncommon.

- Use of the internet and e-mail for **work use** is permitted and encouraged where such use is part of the normal execution of an employee’s job responsibilities and supports the goals and objectives of the organisation;

- Use of the internet and e-mail for **personal use** is permitted where such use is undertaken outside the normal working hours of the employee, or during officially recognised break periods

- *Please note that all employees should limit their personal use of the internet and e-mail during **9am and 5pm, Monday to Friday** because the majority of staff work during this time, which represents the peak period for internet and e-mail traffic*

- Use of the internet and e-mail for **personal use** is permitted where such use does not interfere, hinder or detract from the normal execution of an employee's job responsibilities and does not contradict the goals and objectives of the organisation. The organisation has the final decision on deciding what constitutes excessive use

- Use of the internet and e-mail for **work use** and **personal use** is subject to UK law and any illegal use will be dealt with appropriately. The organisation reserves the right to determine the suitability of this use, which if found in breach of organisation policies, may lead to disciplinary proceedings, dismissal and criminal prosecution;

- Use of the internet and e-mail for work use and personal use will be subject to monitoring for security and/or network management reasons, in line with government guidelines and policies

- Users must not use email for the following:

  1. Advertise for private commercial purposes e.g. selling of goods
  2. Use email for potentially libellous or defamatory purposes
  3. Forward viruses or anti-virus software from outside sources
  4. Any email must explicitly state that the communication is being sent in a personal capacity and not as a representative of PHI.
  5. Remember that emails form part of the administrative records of the organisation and can be disclosed under the **Freedom of Information Act.**

- In addition to internet and email, the following applies to all forms of electronic storage within PHI:

  Staff must not introduce any inappropriate (for example sexually explicit, racially offensive, and homophobic or other unlawfully discriminatory) material onto any organisation equipment or network by any method. Failure to comply will result in disciplinary action.

7. Monitoring

7.1 Email

- Email ***is not*** routinely monitored at PHI, but to the extent permitted by law, the organisation reserves the right to access and disclose the contents of users' electronic communications without the consent of the user. This will only be done when PHI believes it has a legitimate business need and may only take place on authorisation of a member of the Management Team, in consultation with the Head of Human Resources and the Director in charge

- Any user who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so by the IT department

- Electronic mail may constitute "health records" subject to the provisions of the 1998 Data Protection and the Access to Health Records Act. PHI and patients may access, inspect, and disclose such records under conditions that are set forth in these Acts.

7.2 Internet

- Logs are kept by LJMU of all sites visited by staff; and records will be checked if misuse is suspected to ensure that offensive websites are not being visited and to ensure that abuse of the systems is not taking place

- No member of staff is permitted to access, display or download from Internet sites (including Cloud storage) that hold offensive material; to do so, is considered a serious breach of security and may result in disciplinary action, which may lead to dismissal

- Offensive material includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive and other than instances, which demand criminal prosecution, PHI is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet

- The organisation reserves the right, consistent with UK law, to monitor all internet accesses, including but not limited to email and World Wide Web

- No member of staff should consider information sent/received through the internet as his/her private information

- If there is excessive use of the internet the IT Department will raise the issue with the member of staff's manager. If there is evidence that a member of staff has been accessing a site identified as offensive the IT department will inform the relevant Director. A full enquiry will be undertaken which may result in disciplinary action being taken. When a breach is identified, the access of the person(s) involved may be suspended pending the enquiry conclusion

- No organisation information may be emailed, copied or uploaded to websites, blogs, cloud storage or any other form of personal storage except when authorised by IT

8. Email protocols

Email can be a very useful and powerful tool and has become an important and effective means of disseminating and sharing information, especially to large groups of people.

There are, however, some protocols, which need to be considered when using email. Below are some key points, but the list is not exhaustive and common sense needs to be used:

8.1 Good practice

- Always clearly and concisely state the topic of the email in the subject header, but never use a patient or employee name (this may compromise confidentiality)

- Always start your email with a greeting, 'Dear name' is business like and the preferred option, but 'hi' or 'hello' is fine for people you know well

- Always end your email with a 'thank you' or 'regards' as appropriate, otherwise you email may appear abrupt or critical

- If you are asking someone to action a task, always be clear with timescales and avoid emailing something with multiple topics in, as this makes responding more difficult

- Ensure you are kept informed of important organisation emails. HR, Procedure, Legal, IT and Health & Safety matters are sent to all staff by email.

8.2 Bad practice

- Never use bold or capital letters to emphasize a point, as this may be mistaken for aggression; email is different from personal or telephone conversations, where the meaning is naturally picked up from the intonation and stress on words

- Do not use email if a telephone call or brief conversation would be just as effective, you may have heard of the phrase 'management by email' - it can be frustrating to receive an email from a colleague or manager sitting next to you!

- Do not use the CC or BCC functions to 'unofficially' escalate a problem, use the correct management route

- Only send or copy email to the appropriate people, avoid 'round robin' emails and when replying do not use the REPLY TO ALL function unless you have a genuine reason

- Never send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person

- Do not solicit emails that are unrelated to work duties and/or are for personal gain

- Never divulge confidential information

- Before replying to “All” or forwarding email, ensure that you are not sending Personal Identifiable or otherwise sensitive information to unauthorised recipients, by checking lower down the email trail and attachments.

8.3 Internet - Users must not:

- Visit Internet sites that contain obscene hateful or other objectionable material

- Visit commercial chat rooms

- Make or post indecent remarks, proposals or materials on the Internet

- Use the Internet facility for commercial activities, other than in the conduct of organisation business, or for political activities

8.4 E-mail - Users must not:

- Send emails which are harassing, obscene, defamatory or in any other way threatening, intimidating or likely to cause annoyance, inconvenience or needless anxiety

- Create any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material

- Send unsolicited ‘junk’ mail, ‘for profit’ messages or chain letters

- Represent personal opinions as those of the organization

- Solicit e-mails that are unrelated to work duties that are for personal gain

- Forge or attempt to forge email messages; the sender’s name is displayed in each message

- Attempt to read, delete, copy or modify the email of other users without their express permission

8.5 Confidentiality - Users must not:

- Upload, download or otherwise transmit commercial software or copyrighted materials belonging to parties outside of PHI, or PHI itself

- Reveal or publicise confidential or proprietary information, which includes but is not limited to financial information, databases and the information contained therein, computer software source codes

8.6 Security - Users must not:

- Download any software or electronic files without implementing virus protection measures that have been approved by the organisation

- Intentionally interfere with the normal operation of the organisation network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network

- Examine, change, or use another person’s files, output, or user name for which they do not have explicit authorisation

9. Safe Haven Procedures

9.1 Safe Haven media

- Although “safe havens” originally referred to the positioning of fax machines, the meaning has since been expanded to encompass all secure points at which confidential information is received, whatever the media used

- As well as identifying the routine flows of person identifiable information to and from the organisation, the PHI must ensure that there are procedures in place to ensure the information is **received** into a secure and protected point

- All points of receipt should be considered i.e. transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon holes and in-trays for paper information etc

- The PHI must have at least one designated safe haven contact point. Ideally, all information transmitted to the PHI should pass to these contact points. Which must operate in accordance with safe haven principles and the PHI must operate safe haven procedures for all flows of PID

- Access controls and levels to these flows should be agreed by the DPA lead.

9.2 General

A Safe Haven can be either virtual (a set of administrative arrangements) or physical equipment/location. Procedures have been developed to be comprehensive and cover:

- Physical location and security
- Procedures for handling information

9.3 Physical Location and Security

- If the internal mail system is being used to receive person identifiable or sensitive information, it is essential that physical security measures, such as key coded or swipe card entry, are in place to protect information in the post-room, post collection point or similar

- Safe Haven equipment should be secure by way of a lock, keypad or other such method to give restricted access limited to staff who need entry in the performance of their duties

- Access is thus restricted on a "need to know" principle and when granted must be because it is necessary for the member of staff to carry out his or her legitimate activities

- One of the most important features of Safe Haven procedures is the physical security of information and applies equally to paper based and corporate, departmental or stand-alone computer systems

- The area must be protected by an intruder alarm with the combination being changed on an annual basis or immediately a change in circumstances arises. The access code must be changed when a member of staff who had access leaves. If a breach in access rights is suspected the code must also be changed

- Where it is necessary to allow access to this area by people who would not normally be authorised to see Confidential Information, measures must be taken to prevent them gaining sight of Confidential Information

- Under no circumstances is Confidential Information to be left in such a manner that would allow unauthorised access by looking through a window or glass door. As part of security the curtains/blinds in any area containing PID are to be drawn at the end of each day

- All PID held in computer systems must be protected by passwords and staff are responsible for maintaining security of their own passwords, arranging for them to be changed at regular intervals

- Screens likely to show PID must be sited in such a way as to be out of casual view to unauthorised people

- Screens displaying PID must not be left unattended

- Designated fax machines should be located in a secure environment where access is restricted to responsible authorised staff. To enable 24 hour use of the fax it must be locked away securely when the Safe Haven area is not occupied.

9.4 Procedures for handling information

- All Confidential Information, whether it is held on computer or in a manual format, is subject to the Data Protection Act (1998) and all staff are responsible for complying with the Act

- Whatever media is used, the procedure stipulates that the addressee or recipient must acknowledge receipt of the information

- All staff members must be made aware of their own responsibility for ensuring the protection of PID received into a safe haven

- Emails containing person identifiable or sensitive information must be stored appropriately on receipt, e.g. incorporated/stored, and then deleted from the email system when no longer needed. NHSmail is the only approved method for receipt of PID by email, but only if both sender and recipient use an NHSmail account

- A fax machine used to receive person identifiable or sensitive information must be located in a secure environment. Additionally, the faxes should be removed from the machine on receipt. The sender should be contacted to confirm receipt and the fax appropriately dealt with and safely stored

- Recorded telephone messages containing PID or sensitive information, e.g. the names and addresses of applicants phoning for a job, must be received into a secured, password protected voicemail box, so that only those entitled to listen to the message may do so. The department responsible for telecommunications should ensure that a password is required to gain access to messages

- A deputy should be appointed for times of absence, a group password issued or an administrator password made available. If a messages book is used to record messages for absent staff members, this should also be stored securely.

9.5 Fax Messages

- Should it be necessary to transmit PID via fax then this must only be sent to another Safe Haven, or to destination outside where the following procedure must be carried out

- Before transmitting PID via fax for the first or only time, the recipient’s number must be tested. The recipient must confirm that they have received the test message. The recipient fax number must then be stored in the fax machine for subsequent use, if the facility exists

- Fax machines required to be used for transfer of PID must be reported to the Information Governance lead to arrange inspection to ensure that these procedures can apply

- Prepare a fax cover sheet which must contain the following disclaimer:
  > *"The contents of this fax are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, please do not disclose, copy or distribute the information in this fax or take any action on its contents. Any views or opinions expressed are those of the author and do not represent the views of the Public Health Institute unless explicitly stated. The information contained in this fax may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this fax and our reply cannot be guaranteed".*

- Telephone the recipient of the fax to let them know that you are about to send a fax containing confidential information
- Ask the recipient to wait by the fax machine whilst you send the document
- Ask the recipient to acknowledge the receipt of the fax
- Check the recipient's fax number, memory alone should not be relied on when dialling
- It is advisable to pre-programme commonly used fax numbers into the machine's memory. However, a list of speed dial numbers should be prominently displayed next to the machine
- Dial the number carefully
- Monitor the transmission
  - Stop the transmission if there appear to be any anomalies with the transmission
  - If a published fax number turns out to be incorrect, inform all interested parties of the error and amend the list as necessary
  - Obtain a printed record of the transmission where possible
  - No printouts should be left unattended at the fax machine

9.6 Telephone Calls

- A telephone or 2-way radio is not a secure device for transmitting PID

- The use of telephone to communicate confidential data must be restricted to the rare occasion where medical care will otherwise be compromised

- The originator of the call must confirm the identity of the other party and check that they are authorised to discuss Confidential Information. In cases where there is doubt about the identity of the other party the originator is to take the number and dial back to validate the authenticity of the intended recipient

- The Telecommunications Manager is to ensure that all switchboard staff are regularly briefed on the Safe Haven procedures for dealing with telephone calls

- Check that spoken conversations cannot be overheard, for example:
  - Is the reception desk private?
  - Can the reception desk be overheard?
  - Are the offices sound proof?
  - Are out-of-hours arrangements adequate?

9.6.1 Photocopying and Printing

- Managers are to ensure that all staff are aware of the need to minimise the photocopying of PID
- Photocopied data comes under the same control measures as the original document
- There must be a copy of the Copyright Laws near to all photocopiers on site and it is the responsibility of all managers to bring this to the attention of all staff
- Don't leave photocopies or originals containing PID on the machine
- When copying or printing, care must be taken if the machine fails. If it is because of a fault or if paper has run out, remember that the next person to fix the fault or refill it with paper will make your printing appear
- Report photocopier or printer problems
- If you fix a fault or refill a printer, please secure any documents coming out that aren't yours by contacting the originator (if known) or putting them into confidential waste

9.6.2 Mail - Incoming

- All correspondence addressed to a Safe Haven must be delivered to the Safe Haven unopened

- Staff in the Safe Haven are responsible for opening and checking such correspondence and distributing it internally

- Where PID is received it must not be directed to another department without prior knowledge/confirmation that they are authorised to handle such data

- If the recipient is not authorised to handle such data then the element of correspondence requiring their attention should be forwarded with an appropriate statement informing that the Confidential Information has been excluded

9.6.3 Mail – Outgoing

- All outgoing mail involving PID must be directed via the Safe Haven to a designated Safe Haven at the recipient’s location
- Do not use internal envelopes (with folded seal and multiple address panels) to contain PID as these are not sufficiently secure and are prone to mis-direction
- PID transferred by mail must be in sealed envelopes with one clear address on it. A return address must be included either on the envelope or inside to cater for non-delivery

10. Mobile & Teleworking considerations

The aim of this section is to define the procedures to be followed by staff working off-site, taking into account the following:

- **Security**

  Providing access to PHI data opens up the organisation to potential security breaches by enabling employees to download patient information which may not be appropriate unless controlled.

- **Legal liability**

  Misuse of mobile access and storage devices can lead to adverse publicity, legal action and criminal prosecution.

11. General Principles

The internet and e-mail Acceptable Use details in section 6 applies to all PHI employees, as well as people who are not directly employed but who use PHI equipment, IT facilities or data. This Acceptable use is even more important when staff are using mobile storage devices and accessing PHI data remotely.

In addition to the acceptable use of internet and email, the following applies to all forms of electronic storage within or outside PHI:

11.1 Appropriate use

- Staff must not introduce any inappropriate (for example sexually explicit, racially offensive, and homophobic or other unlawfully discriminatory) material onto any organisation equipment or network by any method. Failure to comply will result in disciplinary action.

11.2 Confidentiality

- Staff must not upload, download or otherwise transmit commercial software or copyrighted materials belonging to parties outside of PHI, or PHI itself
- Staff must not reveal or publicise confidential or proprietary information, which includes but is not limited to financial information, databases and the information contained therein, computer software source codes

11.3 Security

- Staff must not download any software or electronic files without implementing virus protection measures that have been approved by PHI
- Staff must not intentionally interfere with the normal operation of the organisation network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network
- Staff must not examine, change, or use another person’s files, output, or user name for which they do not have explicit authorisation

12. Pseudonymisation/Anonymisation

12.1 Definition

Pseudonymisation is the method employed with data for secondary uses for de-identifying person identifier data items. When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets and over time.

Removal of identifiers can also be used; however, this will prevent de-identified records from being linked.

It is possible to produce consistent pseudonyms using techniques, which do not allow the pseudonym to be reversed to permit the identity of the individual to be determined. The use of irreversible pseudonyms allows the linkage of records for the same individual at the same time as effectively anonymising these records.

12.2 General Principles

Confidentiality of Person Identifiable Data (PID) is required as defined in the PHI's Confidentiality Code of Conduct. The security of that information is defined in the Information Security Management Policy. Those documents fully describe the all-encompassing scope of security and confidentiality covered by this procedure.

The Public Health Institute (PHI) will assess all of its data flows to determine the level of pseudonymisation required to still allow its tasks to be completed without unreasonable burdening of processes.

Where possible personally identifiable data (PID) fields will be removed or hidden and replaced with pseudonyms or generalised fields, examples:

- Date of birth – use age or year of birth, or age range
- Data of death – use year of death
- Ethnic Category – use broad categories
- Postcode – use postcode district (first part of postcode)
- Output area – use lower level super output area

Datasets containing PID fields may still be stored but, access may be restricted further if a pseudonymised version would enable most business tasks to be achieved.

Datasets containing PID are restricted to those named on the relevant data sharing agreement, and access to it is monitored. Sensitive or identifiable data extracted from a data asset must only be released in accordance with this Confidentiality Code of Conduct.

Staff will be informed of the processes to pseudonymise datasets.

Commonly used identifiers, such as postcode, which are used for linkage to reference tables (e.g. postcode directory) will not be pseudonymised when there is a need to link these to many different reference tables.

Pseudonymisation will be achieved by applying a salted hash algorithm. It is not possible to un-pseudonymise the hash value to obtain the original code or value.

A short pseudonym will be produced by allocating a random number to the hashed value and storing these in a lookup table.

Keys and salt values will be stored outside the database that holds the pseudonymised data.

13. Agreement with this Code of Conduct

This Code of Conduct will be part of the new starter process, at which time new staff will sign the Confidentiality Code of Conduct compliance agreement form in Appendix 2, a copy of which will be retained in HR. Existing staff are required to sign a copy of the agreement at an IG Training session or during an annual review of staff agreements. There will be time allowed for staff to read this code of practice before signing.

14. Equality Impact Assessment

This policy has been equality impact assessed to ensure that the guidance provided does not place at a disadvantage any service, population or workforce over another. The completed Equality Impact Assessment is shown at Appendix 1.

If you have identified a potential discriminatory impact of this policy document, please refer the issue to the Equality & Diversity Manager at LJMU, together with any suggestions as to the action required to avoid/reduce this impact.

15. Monitoring

The SIRO will discuss and agree with the Data Protection Compliance Group a method for monitoring the dissemination and implementation of this Confidentiality Code of Conduct.
Monitoring information will be recorded in the policy database.

The Data Protection Compliance Group will also monitor the implementation of this, and any subsequent revisions.
Monitoring of activity within PHI is reported regularly to the Data Protection Compliance Group and any variance from the desired levels will be acted upon as appropriate whenever found.

16. References

Department of Health guidance *“Confidentiality: NHS Code of Practice” -November 2003*

All local Data Protection reference material can be found at http://www.PHI.org.uk/governance