PHI | Public Health Institute
LIVERPOOL JOHN MOORES UNIVERSITY

DPA04
Information Security Management System

For all staff at

PUBLIC HEALTH INSTITUTE,
LIVERPOOL JOHN MOORES UNIVERSITY

Document Reference:	DPA04
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	New document	05/06/2013	Geoff Webb
0.2	Draft	Data Retention period added	06/06/2013	Geoff Webb
1.0	Full	changed CPH to PHI	10/11/2016	Mark Whitfield

Contents

1. Introduction

1.1 Approach

The PHI's documented and implemented processes and procedures provide a consistent approach in the provision of systems and services, which take into account the guidance, recommendations and obligations of the following:

- Caldicott - care in confidentiality of patient identifiable information
- Consent to disclosure of patient identifiable information
- ISO 17799 – Information Security Management
- 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
- Information Governance Toolkit
- HCC Audit

1.2 Glossary/Definitions

For the purposes of Information Governance documentation the following definitions apply, some are specific to PHI:

access control	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner
accountability	The property that will enable the originator of any action to be identified (whether the originator is a human being or a system)
archiving case notes	Case notes that need to be removed from the Main Library into the onsite archive area or possibly to the offsite storage facility due to lack of onsite storage capacity
asset owner	individual or organisation having responsibility for specified information asset(s) and for the maintenance of appropriate security measures
audit trail	Data collected and potentially used to facilitate any reconstruction of events within the system
authentication	Corroboration of the origin and correctness of any part of the system
authorisation	The granting of rights, which includes the granting of access based on access rights
availability	Information is delivered to the right person, when it is needed
confidentiality	Data access is confined to those with specified authority to view the data

CRAMM	The CCTA Risk Analysis and Management Method data controller means a person who (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
and	the data are in the form in which they have been or are intended to be processed or recorded with that intention or as part of a relevant filing system or is part of an accessible record
and	processing means obtaining, recording or holding the information or data, including organisation, retrieval, disclosure, blocking, erasure or destruction [Data Protection Act (1998)]
degauss	To remove unwanted magnetic fields and effects from magnetic disks, tape or read/write heads
denial of service	The prevention of authorised access to resources or the delaying of time critical operations
health professional	Any of the following:
	• a registered dentist
	• a registered pharmaceutical chemist
	• a registered osteopath
	• any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends
	• a music therapist employed by a health service body
	• a registered medical practitioner
	• a registered optician
	• a registered nurse, midwife or health visitor
	• a registered chiropractor
	• a clinical psychologist, child psychotherapist or speech therapist
	• a scientist employed by such a body as head of a department
health record	This is any record which consists of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual
Impact	The embarrassment, harm, financial loss, legal or other damage which could occur in consequence of a particular security breach of Information security Protection of information for:
	• availability
	• integrity
	• confidentiality
Integrity	All system assets are operating correctly according to specification and in the way that the current user believes them to be operating
NHS organisations	All organisations providing health care services, including

	health authorities, special health authorities, trusts, general medical and dental practices
password	Confidential authentication information composed of a string of characters
personal data	Data consisting of information that relates to an individual who can be identified from that data (or from that and other information in the possession of, or likely to come in the possession of, the Data Controller), including any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual [Data Protection Act (1998)]
Personally identifiable information	Key data items which may be used to identify a person include:
	• Local identifier, e.g. hospital or System ID Number
	• Address
	• Date of Birth
	• Sex
	• Occupation
	• National identifier: e.g. NHS Number, or NI Number
	• Name
	• Postcode
	• Other Dates, e.g. death, diagnosis
	• Ethnic Group
	[Caldicott Committee: Report on the review of patient-identifiable information -December 1997]
portable equipment	Includes laptop and notebook computers, PDAs, and third generation, WAP-enabled mobile telephones
recovery	Restoration of a system to its desired state following a failure in the operation of the system
risk	The likelihood of occurrence of a particular threat, with the degree of vulnerability to that threat and the potential consequence of the impact if the threat occurs
risk assessment	Comprehensive concept for defining and assessing the potential impact of threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security counter-measures
security audit	A review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures
security breach	Any event that has, or could have, resulted in loss or damage to NHS assets, or an action that is in breach of NHS security procedures
security policy	A statement of the set of rules, measures and procedures that determine the physical, procedural and logical security controls imposed on the management, distribution and

	protection of assets
sensitive personal data	This is data as to the Data Subject's:
	• racial or ethnic origin
	• trade union membership
	• sexual life
	• political opinions or religious beliefs
	• physical or mental health or condition
	• criminal offences, proceedings or convictions
	[Data Protection Act (1998)]
sensitivity	A measure of importance assigned to information to denote its confidentiality
special privilege	Any feature or facility of a multi-user system that enables a user to override system or application controls
threat	An action or event that might prejudice security
vulnerability	A security weakness

1.3 Abbreviations

The following terms/acronyms are used within this document:

The Organisation	Public Health Institute
BSI	British Standards Institute
CCTA	Central Computer and Telecommunications Agency
CD	Compact Disc
CfH	Connecting for Health – The Implementation of National programme for IT (NPfIT)
CRAMM	CCTA Risk Analysis and Management Method
CRS	Care Records Service
CSSR	Councils with Social Service Responsibilities
DOH	Department of Health
DPA	Data Protection Act
FTP	File transfer protocol - FTP is a file transfer protocol for exchanging and manipulating files over a TCP computer network.
IG	Information Governance
IM&T	Information Management and Technology
ISO	International Standards Office
IT	Information Technology
N3	The NHS network - the N3 connects all hospitals and NHS organisations together and is not accessible to anyone who does not have an authorised connection.
NCRS	NHS Care Records Service
NHS	National Health Service
NPfIT	National Programme for Information Technology
PC	Personal computer
PDA	Personal Digital Assistant (handheld computer)
SFTP	Secure FTP - SFTP encrypts data that is transmitted to prevent it being intercepted on the network;

SUS	Secondary Use Services
UK	United Kingdom
UPS	Uninterruptible Power Supply
TLS / SSL	Transport Layer Security / Secure Socket Layer - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers. There are slight differences between SSL and TLS, but they are essentially the same.
VPN	Virtual Private Network - A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
WAP	Wireless Application Protocol (an international standard and a means of viewing data from the internet on a mobile phone)
WEEE	Waste Electrical & Electronic Equipment

1.4 Purpose

An Information Security Management System (ISMS) is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

The implementation of an ISMS is a strategic decision for the PHI.

The ISMS design is influenced by the PHI's needs and objectives, security requirements, business processes and organisational structure. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

In accordance with ISO/IEC 27001:2005 this ISMS adopts the "Plan-Do-Check-Act" (PDCA) model.

This Framework documents the aspects of ISMS that are in place to ensure Information Security and Confidentiality in accordance with ISO/IEC 27001:2005.

2. Scope of the system

These standards, procedures and policies are used as part of the information security management system (ISMS). They are intended to define the practices to ensure the confidentiality and security of patient and staff information.

2.1 Defining patient and staff information

2.1.1 Person Identifiable Data (PID)

"Person identifiable data" relates to information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified.

2.1.2 Sensitive Information

"Sensitive information" can be broadly defined as that which if lost, misdirected or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, data defined as sensitive under the Data Protection Act 1998, for example, financial and security information about an organisation is likely to be deemed "sensitive", as are an individual's bank account details. The following are also included as sensitive information:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Commission of offences or alleged offences

All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. Although each piece of information may be safe on its own, when combined with another it may be possible to identify a person, as shown in the following table:

1. One or more of the pieces of information which can be used along with public domain information to identify an individual	**combined with**	**2. Information about that individual whose release is likely to cause harm or distress**
Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields		Sensitive personal data as defined by s2 of the Data protection Act, including records relating to the criminal justice system, and group membership DNA or finger prints / bank, financial or credit card details / mother's maiden name / National

date of birth and first part of surname]		Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing

2.2 Procedures and supporting controls

Each of the procedures in the following sections is implemented to support the ISMS.

3. Computer User Access

3.1 Objective

To control individual's access to systems to that which is required by their job function. See also Network Security section.

3.2 Registering users

- Formal procedures will be used to control access to systems.
- The registration procedure will ensure that as a minimum:
    - The users full name, department and telephone number are given
    - The users access rights are correct
    - A unique user identifier is used
    - Defined Access levels are agreed with line manager
    - Password procedures and controls are adhered to
- Access privileges will be modified or removed, as appropriate, when an individual changes job or leaves
- Access to systems will be based upon rules which govern relevant level access appropriate to the staff member's job role (role based access), see Access Levels below
- Rule based access will be assessed and regularly audited to ensure no inadvertent breach of security occurs
- All employees of the PHI will be required to sign a declaration form to complete the authorisation process for e-mail and Internet access within the PHI. This declaration expressly states that they have read and understood the policy and guidelines of the PHI, and by using the email or Internet the employee consents to any monitoring of usage that the PHI considers appropriate

3.3 User password management

- No individual will be given access to a PHI system unless properly trained and made aware of his or her security and confidentiality responsibilities
- Passwords must be at least six characters long. Users must keep their passwords secret, never disclose them to colleagues, and if requested to do so report that incident to their Line Manager
- Passwords must be changed at least every 90 days. All new systems must include password ageing to force users to change their password

- Users with authorised access to more than one system may have the same password on all systems to which they have access. This may give different access privileges on different systems depending on job need. It is recommended however that where multiple access is required the user must choose a password with sufficient complexity of structure to reflect the confidentiality of data on those systems

3.4 Change of user requirements

Changes in requirements normally relate to an alteration to applications used, or changes to network access. Requests for change must be made in writing (email or hard copy) by the newcomer's line manager or by HR in the same way as a New User request.

IT will maintain a record of all these Requests for Access to Computer Systems with the category "Change Requests".

3.5 Change of password

Where a user has forgotten his/her password, the Service desk is authorised to issue a replacement.

Upon receipt of such a request the Service desk will:

- Ensure the request is logged
- Confirm the identity of the user by asking a security question
- Issue a temporary, single use password which will require the user to set up a formal password upon first log-on

3.6 User Privilege management

"Special privileges" are generally those allowed to System Managers, System Administrators or systems programmers, allowing access to sensitive data (i.e. Passwords).

The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached and therefore **must be considered only in exceptional circumstances.**

3.7 Access Levels

- The role of a person in relation to a computer system will determine which of the predefined and approved access level is required
- User access rights are subject to granular control to ensure that staff have access to the information they need to use. For example, Administrator rights, Supervisor level, read only
- Access must be granted at a level that enables the person to carry out their role whilst not giving excessive or inappropriate access rights

- Individual systems must have written policies and procedures (approved by the DPA Compliance Group) that require user registration and logon ID and password

3.8 Email and User Account Deletion

3.8.1 Leaver processing responsibilities

The Human Resources department is responsible for:

- The production of the leavers list on a regular basis to an agreed format and frequency
- The modification of any internal systems / forms to support the process and authorise the actions identified
- The leavers list is the primary trigger for the IT department to initiate the process of account deletion for a user. It is essential, therefore, that the list must be timely and above all accurate. Incorrect inclusion of a current staff member in the leavers list could result in significant loss of data

The User must:

- Assist the service / departmental manager in reviewing the files and e-mails held of the system to determine actions to be taken before the accounts are deleted
- Not perform bulk deletion of files and e-mails from their accounts, in preparation for leaving the PHI or transferring, without prior agreement from the service / departmental manager
- The user is solely responsible for copying personal files they wish to retain to appropriate media. Failure to do so will result in those files being deleted

The service / departmental manager:

- Must review with the user, the files and e-mails held on the systems to decide whether they are to be retained
- Identify any generic / departmental accounts held in the name of the user and notify the IT department, at least 1 week prior to the leaving date, of the name of the new “owner”
- If business files are to be retained they must decide on the time required to transfer these files / e-mails to a secure location
- Decide the name(s) of any individual(s) who will need access to the user account to carry out the necessary file management
- Notify the IT Department of the need to transfer files, the time required for the process and the names of the individual(s) who will require access to the user account – failure to do so will result in the files being deleted 30 days after the member of staff leaves
- Ensure that the user is aware that they are not to bulk delete files without prior agreement
- On completion of the file management notify the IT department

The IT Department:

- Must, on receipt of the leavers list and any notification from the service departmental manager, initiate the user account deletion process as defined in Appendix 2 or 3 (whichever is appropriate). Premature deletion of user files and/or e-mails could result in significant data loss for the PHI

3.8.2 Staff transferring within the PHI

- The service / department manager in the area where staff are transferring from must initiate discussion with the user, prior to the leaving date – the purpose being to establish the nature and quantity of files held in the user accounts
- The service / departmental manager must identify any generic accounts that are "owned" by the user and designate who is required to take over such ownership when the User transfers
- The service / departmental manager must decide which business files and e-mails are to be retained and identify those who will carry out the necessary file management and whether the routine 30 days will be sufficient time to complete the task
- The user must identify and copy any personal files from the systems. Any files removed must be agreed with the service/department manager
- Access to files, folders and systems for the user in the area they are transferring to is handled in the same way as a new starter

3.8.3 Staff Leaving the PHI

When the Staff Leaver Form is completed for a member of staff who is leaving, this must be the trigger for a number of events:

1. The Human Resources function must produce a leavers List which shows only those staff who have left or are leaving the PHI. This must show the name of the member of staff, the role, the department or specialty they work in and the date of leaving. A copy of this list must be forwarded to the IT Help Desk
2. The service / department manager must initiate discussion with the user, prior to the leaving date – the purpose being to establish the nature and quantity of files / e-mails held in the user accounts
3. The service / departmental manager must identify any generic accounts that are "owned" by the user and designate who is required to take over such ownership when the User leaves
4. The service / departmental manager must decide which business files and e-mails are to be retained and identify those who will carry out the necessary file management and whether the routine 30 days will be sufficient time to complete the task
5. The user must identify and copy any personal e-mails or files from the systems. Any files removed must be agreed with the service/department manager
6. The IT department will follow a pre-defined procedure for deleting accounts that allows for:

- Providing advice to the user, where necessary, on the process for copying files and/or e-mails from the system to portable media.
- Service / departmental files to be accessed, tidied and copied to an appropriate secondary location prior to deletion

The stages in the procedure are illustrated fully in the Appendix diagrams and summarised below:

- **Network files and E-Mail Accounts – Deletion Process**

Following the review between the service / departmental manager and the leaving user, where a decision is made that neither files nor e-mails need to be retained then the procedure outlined in figure 1 must be followed. It must be noted that a "cooling off" period of 30 days has been introduced to allow time for the situation to be reviewed.

- **Network files and E-Mail Accounts – Retention Process**

Following the review between the service / departmental manager and the leaving user, where it has been decided that files or e-mails need to be retained then the procedure outlined in figure 2 must be followed. It is important to note the responsibilities.

4. Network Security

4.1 Objective

This section defines the Network Security Procedures for the PHI.
It applies to all business functions and information contained on the network, the physical environment and to relevant people who support the network.

It sets out the processes for the protection of the confidentiality, integrity and availability of the network.

It establishes the security responsibilities for network security.

4.2 Scope and Definitions

4.2.1 Scope

The section provides governing principles for data security for internal and all inter-organisational networking between PHI systems and with non-PHI systems.

It is intended to establish a clear set of rules that will ensure the availability and security of confidential data for which the PHI has a statutory responsibility.

The procedure covers all aspects of the network described below.

4.2.2 Definitions

The network is the infrastructure upon which a collection of communication equipment such as servers, computers, printers, and modems, has been

connected together by cables or other wireless means of connection. The network infrastructure is made available to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

The term "external data communications" refers to any electronic data communication between computers within the PHI and those outside the PHI. It applies to both existing and future links.
Existing links include access to the Internet, Electronic Messaging, and System Support.

4.3 Aims of Network Security

To ensure the security of the network, the PHI will:

- Ensure availability
- Ensure that the network is for authorised users.
- Preserve integrity
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the PHI's information assets.
- Preserve confidentiality
- Protect assets against unauthorised disclosure

4.4 Internal Links

The PHI has an extensive Local Area Network (LAN) which links users in all locations to enable access to the server based documents and systems. Access to the network is by password protected user account, described in the Computer User Access Management section.

4.5 External links

There is access to the internet via the network.

4.6 Internet and Email Guidance

4.6.1 Acceptable Use

Staff have certain duties and responsibilities regarding the appropriate use of the internet and email. These include ensuring that emails are read and acted upon, then filed or deleted, not accessing inappropriate internet sites and not abusing the permitted personal use of either the internet or email.

4.6.2 Global emails

All emails to be sent to a global distribution must only be done by the Communications Department. Global emails must not contain Person Identifiable Data.

4.6.3 Monitoring

If staff are found to be accessing sites inappropriate to their post this may be considered as gross misconduct.

Access to web sites and the length of time spent on the internet may be monitored and reported on by IT. Users found to be accessing recognised undesirable sites, or making excessive use of the internet for personal purposes will have access rights withdrawn immediately and may be subject to PHI disciplinary procedures..

If access rights are withdrawn users will receive a message when attempting to access the Internet. A report will be sent to their Manager.

4.6.4 Personal Use of the Internet

4.6.5 Use of the internet for personal use is permitted where such use is undertaken outside the normal working hours of the employee, or during officially recognised break periods.

Use of the internet 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.

4.6.6 Blogging and Social Network websites

The use of blogging and social networking websites by an organisation's employees can expose that organisation to information risks, even where these sites are not accessed directly from work. Whilst there is nothing new about the information risks, what has changed is the availability of high capacity broadband, the popularity of Web2.0 sites and the rapid growth of internet enabled devices such as mobile phones, blackberries etc. This has resulted in significant awareness and uptake of these websites from home, from work and when mobile.

Potential threats that staff must be aware of:

- Unauthorised disclosure of business information and potential confidentiality breach
- Blogging and social networking sites provide an easy means for information to leak from an organisation, either maliciously or otherwise. Once loaded to a site, organisational information enters the public domain and may be processed and stored anywhere globally
- In short, organisational control is lost and reputational damage can occur

4.6.7 Malicious attack associated with identity theft

People often place a large amount of personal information on social networking sites, including details about their nationality, ethnic origin, religion, addresses, date of birth, telephone contact numbers and interests. This information may be of use to criminals who are seeking to steal identities or who may use the information for social engineering purposes.

4.7 Internal Security

In order to provide a second level of security the LJMU also has its own secure gateway - sometimes referred to as a "Firewall" - which controls the flow of data between the PHI and the Internet.

This is administered by IT and, in addition to providing security, monitors traffic from and to the network.

This monitoring includes such information as who uses the link, for how long and to what sites. It also monitors incoming data downloads (particularly from the Internet) to ensure virus protection and can be used to block undesirable material.

4.8 Conditions and Requirements

4.8.1 Network Connection

Connection to the outside world will be through the LJMU network.

4.8.2 Data Protection

The normal statutory obligation on the handling of electronic data applies. It is the personal responsibility of all staff to ensure compliance. Further details about the Data Protection Act (1998) are contained in the DPA Confidentiality Code of Conduct.

5. Network Remote Access

5.1 Objective

To control access to the PHI computer systems by individuals outside the normal environment of the PHI.

5.2 Access

Access to the LJMU network gained from outside the PHI's environment by the use of VPN (**Virtual Private Network)** connectivity to the core servers and extranet which does not use VPN must be monitored.

There are numerous methods of connection, both fixed (office based and home broadband networks) and mobile (Wi-Fi, GPRS and 3G) networks for connection to the PHI file servers, which must be monitored and controlled.

As well as the method of access there must be control on the type of devices that are connected to the LJMU network. It is recommended that staff are obliged to use only PHI supplied or approved devices.

5.3 Transfer of data

Data is frequently downloaded to laptops and home-based computers so that staff can work locally without the need to maintain a network connection.

Whilst this may be convenient there are two major risks that must be minimised:-

- Loss of the data held locally

  When data is taken from the server and is used locally it must be backed up frequently by copying to an external device, or by uploading it back to the server. To be completely safe all access to PHI data should be by accessing the servers via either direct or remote connection as described earlier so that no data needs to be held locally on the laptop.

- No referential integrity

  As there is no automatic control checking files in and out of server folders it is possible for two people to be working on separate downloaded copies of the same file. Action must be taken to investigate a solution to this problem, or establishing a policy that all PHI data should be accessed on the servers via either direct or remote connection as described earlier so that no data needs to be held locally on the laptop.

It should be made clear to staff that using copies of PHI data on a laptop is a risk for the reasons stated above and that the laptop must not be considered to be a backup device for the server folders.

Data taken off site, via laptop, network or removable media must conform to the Caldicott Principles.

6. IT System backup

6.1 Objective

To define the safe and timely copying of computer system data to a medium from which it may be restored later if required. LJMU carries out backups of Shared Drives.

6.2 Server backup

To allow data essential to the business of the PHI to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems. In order to achieve this there must be set procedures to cover:

a) copying of data to a medium which can then be stored in a secure place (backup)
b) retrieval of data from copy made on the medium in a) above (restore)
c) secure storage of media containing the data copies made in a) above
d) recording of details about the media and what data it stores to facilitate the easy and correct identification of a particular item of storage media when it is necessary to retrieve data from it, as in b) above
e) testing the quality of the back-ups made in a) above both by log checking, verification techniques and by test retrieval of data from an item of storage media

It should be noted that if data is stored on the PC rather than the network servers it will not be part of data recovery procedures.

The PHI requires that:

- All central systems will have daily backup regimes formalised in a job run manual. Such backups will have a minimum of five days cycle before media is overwritten.
- All networked PCs will use the designated drives on the server.
- Under no circumstances should data be stored on the local drives of PCs which are connected to the network. Removable media (CD's, USB sticks etc.) must never be used to store data, but only for transferring data where that is permitted
- USB sticks must be approved by IT and encrypted

Detailed arrangements for Systems Backup can be found in the System Backup Procedure document.

6.3 PC/Laptop backup

There must be an automated backup process to ensure a high level of data security and integrity. Software that prompts laptop users to make backups and upload files previously downloaded should be implemented and staff must be made aware of their obligations to follow the backup procedures.

7. Virus Control

7.1 Objective

To define the process of protecting the PHI computer systems from malicious software attack.

7.2 Definition

Computer Viruses are the main source of malicious software encountered and recorded that effect Information Systems. They are distributed in many ways, via physical media interchange, but more dangerously electronically as programs and attachments. Virus detection and cleansing packages are common and effective against the common and known viruses.

The best protection from virus attack is through:

- Good security awareness procedures that are enforced
- Education and awareness of all staff
- Strict software licence and usage policy
- Good network and system access control systems and procedures
- Formal change management processes for Information Systems

The purpose of this procedure is to protect the integrity and operation of all software and information used and held on Information Systems from malicious software attack.

7.3 Scope

All IT systems must employ approved processes to prevent and detect malicious software attacks by:

- Implementing Virus detection and prevention measures on all IT assets vulnerable to attack

- Providing staff awareness updates where necessary to promote continued vigilance by staff

- Managing all assets to ensure correct operation, detect any changes and additions to the software loaded and configuration changes

7.4 Recording Anti Virus Software in use

Anti Virus Software in use is maintained by LJMU CIS.

7.5 Controls

The Procedure is enforced by LJMU CIS, implementing the controls and associated procedures defined in this section:

- A recognised industry standard virus detection package must be used on IT systems

- File storage systems must check for virus corruption before storage

- All corporate servers must have virus detection operational and running at all times

- Desktop systems must have virus detection software loaded and enabled

- Consideration must be given to virus detection on Email gateways

- Consideration must be given to virus detection on network gateways

- On-line virus library updates must be used to provide regular updates

- On-line virus dictionary updates must be transmitted to user systems when they become available

- All mobile (Laptop) users must be automatically updated on attachment to the network. Staff using their own equipment or Mobile and stand-alone PC users are responsible for ensuring virus updates are made at least once a month

- Users who disable or reconfigure the PHI/LJMU virus detection software will be subject to action under the LJMU disciplinary procedure

7.6 Staff Awareness

- The IT department must provide staff awareness material for Virus Control and other security issues

- Virus control awareness must be included in the staff induction process for those staff working with IT systems

- Managers must ensure that all staff are aware of this Procedure and responsibilities under it including the fact that non-compliance will be subject to action under the LJMU disciplinary procedure

7.7 Use of Software

- Only software authorised by the PHI may be loaded and used on PHI equipment

- Unlicensed software **MUST NOT** be loaded and used on PHI equipment.

- Shareware and freeware software **MUST NOT** be loaded and used on PHI equipment

- The downloading of any software must be authorised and approved by the IT department

- All critical systems must be scanned daily by automatic processes which are updated regularly (also automatically), as new virus definitions and scan engines are released

- Users who load and /or use unauthorised software onto PHI equipment will be dealt with in accordance with the LJMU disciplinary procedure

7.8 External Media

All external media, for example CD Rom, USB Memory sticks and transmitted data, must be supplied/authorised by IT and checked for virus off-line before being loaded onto a PHI/LJMU IT system. See also Transporting Sensitive Data and Mobile Data Storage sections.

Users who load unauthorised media onto a PHI/LJMU IT system will be dealt with in accordance with the LJMU disciplinary procedure.

8. Information Asset Management

8.1 Objective

To maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the PHI.

8.2 Purpose

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 the operation and continued success of the PHI.

The PHI acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.
A requirement for ISO/IEC 27001:2005 compliance is to have a clear understanding of the information assets involved and to document these in an Information Asset Register, which forms a key input to Risk Assessment.
It is essential for compliance with ISO/IEC 27001:2005 because it is the foundation for the selection and deployment of security controls.
The purpose of this Information Asset Register is to identify the different types of information processed, stored and communicated by the PHI.

8.3 Definitions

8.3.1 Assets

The Information Asset Register includes all information assets relevant to the Information Security Management System (ISMS) and details the classification and ownership of each of the information assets.

It is important to ensure that the Information Asset Register is kept under control and updated as necessary. The Information Asset Register should be updated every time the details of one of the information assets are changed.

This document outlines the standards and procedures for the recording, control, auditing and disposal of information assets. It also includes standards and procedures for change control and hardware updates.

An information asset can exist in several formats both in terms of the physical media on which the data is stored and in terms of whether it is permanently or temporarily stored. This affects the security controls that may be applied as a result of the Risk Assessment e.g. paper documents may be locked in a cabinet whilst files stored on a network drive may require the setting of system access rights for protection.

Major information assets are those that are central to the efficient running of departments of the PHI for example business, finance or personnel data. Information assets will also include the computer systems and network hardware and software that are used to process this data. Non-computerised systems should also have an asset register containing relevant file identifications and storage locations.

There are six major categories of information asset:

- **Information** - Databases, system documents and procedures, archive media/data etc
- **Software** - Application programs, system, development tools and utilities
- **Physical** - Infrastructure, equipment, furniture and accommodation used for data processing
- **Services** - Computing and communications, heating, lighting, power, air-conditioning used for data processing
- **People** - Their qualifications, skills and experience in use of information systems
- **Others less tangible** - For example, the reputation and image of the PHI

As these categories suggest information assets are not necessarily objects. Business processes and activities, applications and data should all be considered as information assets; however, their importance to the PHI may vary.

8.3.2 Information Asset Owners

The word ‘owner’, when used in this requirement, is taken from the ISO/IEC 27001:2005. It should not be confused with the term ‘data owner’, as used by the Data Protection Act 1998. The standard defines an owner as a member of staff senior enough to make decisions concerning the asset at the highest level. Hence, the Director with responsibility for Information Governance may be considered the owner. The owner can assign day to day responsibility for each information asset to an administrator or manager, and this should be formalised in job descriptions.

The role of the asset owner is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The asset owner will also be responsible for providing or informing written reports to the designated Risk lead annually on the security and use of their asset.

It is important that “ownership” of information assets is linked to a post, as opposed to a designated individual, to ensure that responsibilities for the asset is passed on should the individual leave the PHI or change jobs within it.

8.3.3 Asset register

Information assets should be documented in an asset register. In practice, a number of asset registers may exist (e.g. departmental, Freedom of Information Act), and many will be ad hoc. In order to establish corporate coherence it may be possible for a single asset register to be created for the PHI. It is essential that all critical information assets are included in this asset register, together with details of the “asset owner”. To improve its usability and maintainability, the information asset register may be service, rather than location, based.

The best type of asset register will link all the categories listed above. For example, the entry for a physical asset such as a file server will include its physical location, what software and information is included on it, those responsible for the maintenance of the file server, how to contact them if something goes wrong, if it is linked to an Uninterrupted Power Supply (UPS) system, and any Business Continuity Plans for recovery. Details of a business process, such as a particular employment position, should be seen as an asset, with job description, location in organisational structure, qualification/experience necessary for the position, employee development plan, etc. all linked to the asset.

The Information asset owner should also be aware of what information is held

8.4 Document Classification

8.4.1 Asset Inventories

It is important to standardise the hardware asset register, using an easy to read, and track naming convention. Each hardware device will have an asset tag placed in a visible location, no tags should be placed over any existing serial numbers.

8.4.2 Hardware Inventory Registers

All hardware devices are entered onto an electronic asset register accessed only by staff within the Informatics Services Department. The following information will be collected relating to equipment purchased though the IT Department:-

- Manufacturer, product description and model/serial number
- Any purchase/lease information where available, (details of lease agreement to be referenced)
- Owner of equipment

8.4.3 Component Data PC/Notebook/Server

- Manufacturer, product description and model/serial number
- Software installed, manufacturer, product and version
- Configuration, Build
- Business Owner

8.4.4 Inventories

All Asset registers must be reviewed every 6 months, but constantly updated when changes occur, by the IT Support Manager / Deputy Head of IT
A network audit can be carried out at any time using products such as Audit Wizard, where software can look at the following information**:**

- Category (PC, Server, Printer)
- Make (Dell, Compaq etc)
- Model (Dell Inspiron)
- Hardware
- Bios (Date, Manufacturer, Version)
- Number of drives including letters (Type, Size, Label, Free Space)
- Environment Strings

- Graphics (Adapter, Colour Depth, Monitor, Resolution)
- Memory (Type, Size, Number, Capacity)
- Motherboard (Processor, Bus type, Co-processor, Speed, Sockets, Voltage)
- Network (IP Address, Logon Client, MAC Address, Network Adapter, Protocols, User Name)
- Peripherals (All attached peripherals)
- Sound, Video and Games Controllers
- USB (All Devices)
- User information
- Software installed (licences)

The software can also check internet history and cookies installed on the machine.

Controls and spot checks may be periodically carried out at any time. Asset tags must verify the identical information in accordance with the Asset register; any missing or damaged tag must be replaced immediately. If any part of the asset register does not match the piece of hardware/software/data then changes should be made and recorded. Any unlicensed software identified must be removed immediately and cannot be reinstalled until a license is purchased.

8.5 Removal, Re-use and Disposal of Assets

Any equipment considered out of date, redundant or inoperable, beyond cost effective repair, will be dealt with in the following manner.

The IT department must be consulted when any piece of equipment is deemed to be obsolete or redundant so they can make the decision as to whether it can be used elsewhere within the company. This must be done prior to its removal.

If no alternative use has been identified then the piece of equipment must be completely sanitised, including the destruction of disks, prior to disposal. All asset tags will be removed and the relevant register amended.

Media will be disposed of in a manner appropriate to the media concerned. These will comprise:-

- HARD DISKS - by means of rendering them unreadable, such as degaussing

- FLOPPY DISKS, TAPES and CD'S – by physical destruction under guidance of IT

- Documentation – by shredding

8.6 Software Licensing

The majority of software used by the PHI is covered by corporate license agreements with the vendors or under natural license agreements.

It is the responsibility of the IT Systems Manager to ensure that the PHI has the correct number of licenses for software that has no agreement in place.

All licenses must be kept by the IT Systems Manager in a filing system setup as part of the IT Department documentation.

Under no circumstances must employees download or bring in unlicensed software. If there is a requirement to test new software it must first be installed in a staged environment and, once approved, the IT Systems Manager must ensure that adequate licenses are purchased to support the PHI's needs.

If users receive messages to update to the latest version of a software product the appropriate action is to contact the IT Service desk for advice.

8.7 Asset Classification

8.7.1 Principles

Information assets represent a valuable resource to the PHI and as such require protection. However, the information held and used by the PHI varies greatly in its value and, as such, it may be treated with varying degrees of security. In order for this to be workable it is necessary to establish a clear classification scheme to apply to all information. This classification scheme allied to removal, disposal and handling procedures etc will provide guidance to staff in the effective management of information.

It is the responsibility of all employees to ensure that all data created, stored or used by them has the correct classification associated with it. If documents fall into the restricted or confidential categories then it is the employees' responsibility to ensure it is labelled and handled correctly.

8.7.2 Classification Scheme

Work should be undertaken to find an appropriate classification scheme to be adopted by the PHI in due course.

8.7.3 Equipment Maintenance

One threat to the PHI's computer-based systems (and hence its business continuity) is that of equipment breakdown or failure. To overcome this, an equipment maintenance strategy has been developed. The servers and other

equipment are, generally, extremely reliable so it is not necessary to have regular, planned maintenance carried out by manufacturers' engineers.

The strategy adopted is a combination of built-in redundancy, call-out maintenance contracts and in-house repair – with equipment still under warranty being repaired or replaced by the supplier or manufacturer as required.

Further details can be found in the Equipment Maintenance and Management section.

9. IT Equipment Maintenance and Management

9.1 Objective

To describe the procedures that should be in place to maintain continuity of IT Equipment and Services.

The PHI demands that threats to its IT services are taken into account in contracts and suitable controls and that there are strong links between this and Business Continuity Plans.

In addition to providing contingency for a major disruption to services there is also a large benefit to be achieved in terms of continued service by the appropriate use of preventative maintenance and equipment management.

This section describes the operational aspects of those maintenance procedures that must be in place.

9.2 Scope and Definitions

The management and maintenance of all IT equipment and systems is required as part of this Information Security Management System.

9.3 Recommended Scheduled Maintenance

Maintenance contracts can be established with third party organisations or internal departments. Maintenance contracts with internal departments should be agreed in the form of a Service Level Agreement (SLA).

Maintenance contracts for key equipment should take account of the effects of downtime on services. A range of contractor callout times may be available (for differential fees, of course). For example, response times of less than one hour, four hours, eight hours, etc. The risk assessment plan for the equipment should help determine what conditions are required. All servers should be regarded as critical items of equipment, which should be reflected in their maintenance contracts and support. Response times should also take consideration of the day and time. If the equipment is required 24/7 then the contract needs to reflect this. Callout responses based on Monday-Friday 9am-5pm clearly will not do in this case.

The option of loans of replacement equipment should be considered for key items. Replacement components or facilities should be made available for all

key assets and alarms fitted where possible. All items have limited life spans so equipment such as backup tapes should be allocated a reasonable usage period and replaced and securely disposed of in that time.

It will not be possible or desirable to stock emergency spares for all information processing facilities and ancillaries. However, risk assessment and business continuity plans should identify the areas of greatest risk, and what spares are likely to be needed. For example, network cabling and junction boxes are particularly prone to accidental damage. They are likely to be stored on-site for use in emergency situations. However, more substantive items may not be readily available. In such cases the business continuity plan should ensure that they can be delivered in pre-determined times. Contracts with third parties supplying equipment should include times for delivering spare components.

The department holding the maintenance contract should ensure that the person responsible for the equipment knows what date the contract expires. All maintenance actions (repairs, upgrades and replacements etc.) should be arranged and agreed with the member of staff responsible for the equipment and records kept of all preventative and corrective actions.

9.4 Maintenance Procedures in place

A list of all existing contracts and maintenance agreements for IT equipment and other equipment maintained by IM&T must be kept up to date.

Equipment covered	Location	Agreement Starts	Agreement Ends	Company

10. Access to Secure IT Areas

10.1 Objective

This section lays down the security arrangements required to reduce the risk of unauthorised access to critical IT systems and equipment housed within designated IT secure areas.

10.2 Designated IT Secure Areas

The designated IT Secure Areas in the PHI are as follows:

- IT Computer Equipment Room (across the PHI sites)
- IT Storage Areas
- Network Hub Cupboards (across the PHI sites)

10.3 Access

- Responsibility for access to each IT Secure Area will rest with the IT Support Manager

- Unrestricted access to IT Secure areas will be confined to authorised designated staff only whose job function requires access to that particular area/equipment

- Each department manager/system administrator, with responsibility for a secure area will maintain a list of current designated staff who have appropriate authorisation and ensure that security procedures are maintained

- Departments housing network hubs not contained within computer rooms must ensure that the areas are locked at all times and are restricted to departmental and IT staff only. This equipment must be protected against accidental or malicious damage

- Areas secured by coded keypad locks must have their codes changed monthly to ensure that they are not compromised

- KEYPAD CODES, KEYS OR DETAILS OF ANY OTHER PHYSICAL CONTROLS MUST NOT BE GIVEN OUT TO ANY UNAUTHORISED PERSONNEL

- All visitors must be accompanied to the area and must sign in and out of the visitors log book. The log book will be made available at all times to the IT Manager and will not be removed from the area

- Access should only take place with prior arrangement and on authentication of personnel. No equipment/data should be removed from its site without prior authorisation by the IT Manager or other delegated responsible person

- All other unauthorised access including third party support agencies must be controlled through the maintenance of a visitors log book, recording the details of the duration and purpose of the visit

11. Mobile Data Storage and transfer

11.1 Objective

To define the methods of transferring sensitive and Person Identifiable Data (PID) with due regard to security and confidentiality.

11.2 Background

There are frequent reports about data losses throughout the UK. Breaches happen when information that uniquely identifies an individual is made publicly available.

To completely resolve the problem and remove all risk to confidentiality it would be necessary to stop transferring data completely.

This is not a practical course of action so the short term answer is to take steps to ensure that personal data is protected. Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone must also be encrypted. This is now a requirement across all public sector organisations set by the Cabinet Secretary.

11.3 Data encryption techniques

Encryption is the process whereby data is effectively scrambled according to a complex algorithm or cipher making it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

The result of the process is **encrypted** information (in cryptography, referred to as ciphertext). Encryption is widely used in protecting information within many kinds of information systems. It can be applied to files of data, complete disks (such as a PC hard disk) or external devices such as USB Memory sticks.

All Laptops and Memory sticks used by staff to store PID must be provided by IM&T because they have encryption built in which cannot be turned off.
You cannot write data to a USB device unless it is one from IM&T, although you can read from one to allow for the use of presentations etc.

Take care of passwords that protect access to confidential information on portable devices

11.4 Transferring Data

A variety of policies, tools and technology solutions have been developed to handle all organisational information – in particular the personal and sensitive information of patients and employees. In this way, the PHI can ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

These guidelines provide a quick reference, focussing on recommended solutions to minimise the risk of losing person identifiable data.

11.5 Multiple record transfers

Multiple is defined by DOH as being groups of more than 50 records. This could be a database with multiple entries or an electronic folder, disc, or paper records containing more than 50 records about individuals. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of information.

Security and confidentiality of large numbers of records may differ from single records due to the methods of transfer likely to be used.

Most importantly in all cases where more than 50 records are being transferred, the recipient must have signed up to the PHI's Overarching Information Sharing Protocol and there must be an agreement under the Information Sharing Procedure]), in which the recipient agrees to comply with our Confidentiality Code of This agreement will ensure that the assurances we have given regarding security and confidentiality are honoured by the recipient.

11.6 Information transfer methods

The way in which information is transferred is key to determining and ensuring its ultimate safety from interception, loss or corruption. Such methods may include fax, mail, emails, tapes, floppy discs, laptops & handheld computers, optical discs - DVD & CD-ROM, solid state memory cards, memory sticks and pen drives.

The use of any of these items will constitute a risk.

When communicating patient related data the minimum amount of PID necessary must be used. The principles of the Data Protection Act 1998 and the Caldicott guidelines, defined in the Confidentiality Code of Conduct, must be adhered to at all times.

Methods of transferring PID are explained in the following section.

12. Procedure for transferring data

12.1 Objective

To describe each method of transferring data and define the safety measures to be carried out when doing so.

12.2 Fax Transmission

Transmission of person identifiable data via fax is not recommended. However where there is no alternative safer method and the risk of loss of data is outweighed by the risk to patient care then that risk must be assessed and the appropriate action taken.

Designated Safe Haven fax machines for the receipt of confidential information must be located in a secure environment where access is restricted to responsible employees. Only those fax machines listed in the Safe Haven Procedure are authorised to receive person identifiable information.

Should transmission of personal clinical information via FAX be unavoidable then details such as name, address, date of birth and any other items that could identify the data subject should be redacted if possible.

For transmitting confidential Information via FAX on a regular basis the recipient's number must be tested prior to sending, programming recipient numbers into the fax memory. The recipient is to confirm that they have

received the test message. This action precedes the sending of faxes and is designed to reduce the risk of misdialling.

12.3 Telephone Calls

A telephone is not a secure device for transmitting Confidential Information.

Use of the telephone to communicate confidential data is restricted to the rare occasion where medical care would otherwise be compromised.

The caller 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 caller the other party must take switchboard details and call back to verify their authenticity.

Check spoken conversations cannot be overheard, for example:

- Is the reception desk private?
- Can the reception desk be overheard?
- Are the consulting rooms sound proof?
- Are the out-of-hours arrangements adequate?

Be aware that two-way radios are not secure.

12.4 Mail

12.4.1 Mail - Incoming

It is essential that when communicating with people or organisations outside the PHI, they are made aware of the correct address to write to.
Where person identifiable data is received in error it must not be forwarded to another department without prior confirmation that it is appropriate to do so.

It is not appropriate to leave any incoming mail in a mail delivery location that is not secure as it could contain person identifiable data.

12.4.2 Mail – Outgoing

All outgoing mail involving person identifiable data must be properly addressed to the recipient's location.

In a Safe Haven or other departments authorised to hold PID it is required that all such data is secured in a locked cabinet when not in use.

No PID is to be placed in a position that will allow visitors to gain access.

No PID may be retained for a period longer than is necessary to comply with statutory or local management requirements.

It is not appropriate to leave outgoing mail containing PID in a mail collection location that is not secure.

12.5 Email Transmission

Users must not communicate any PHI-related business, including the transmission of PID via personal email/webmail accounts. If you are required to transmit data, the only safe way is through secure emails. PHI email (name@ljmu.ac.uk) is only secure within the organisation, not for sending any information to an email address outside the PHI because it goes via the internet in an unsecured way.

12.6 Secure File Transfer

12.6.1 Purpose

Secure File Transfer (SFT) is designed to replace the following physical media transfers often sent by courier or hand delivered, often at great expense & effort:

- CD or DVD
- Memory sticks, USB pen drives
- Printouts

12.6.2 Permitted Use

The main uses of SFT are:

- Transfer of personal or other sensitive data
- Not a “blue light” service
- Available as an option in critical situations

PHI have set up a Microsoft Sharepoint secure FTP site for the secure exchange of PID data. The link for external agencies is: https://extshare.ljmu.ac.uk/dept/hea/PHI/PHI-mon/default.aspx A registered list of all PHI employees and staff at external agencies with access to the Sharepoint dropbox are held by the Monitoring Team.

12.6.3 Working at Home

All staff who use PHI equipment at home or who may use their personal computing resources to connect to networked services of the PHI are subject to these requirements. Refer also to the LJMU HR Home Working Policy

The IT Support Manager is responsible for the local definition of network, infrastructure and PC information security requirements and for the supply and configuration of all computing equipment provided by the PHI. This will include network connectivity and support for approved services.

Where, exceptionally, agreement is provided that a home worker may use their personal computing resources for a business purpose of the PHI, the IT Support Manager must be satisfied that the resources concerned are configured appropriately, that PHI security measures are implemented and operating correctly and that no unacceptable information risks exist.

The IT Security Manager is responsible for ensuring that a home risk assessment survey is conducted where necessary and for the identification of any necessary improvements or controls that affect the proposed home work area. In addition, the IT Support Manager will provide guidance to the home worker on all relevant security policies and responsibilities.

A home risk assessment survey will be necessary when an individual who regularly works from home, (defined as at least 6 times during a year), has access to:

a) Documents protectively marked as 'confidential' or above in accordance with central government guidelines (not applicable in the NHS);
b) Other commercially or otherwise sensitive documents;
c) Any sensitive person identifiable information about patients or staff;
d) Person identifiable information about patients or staff deemed non sensitive but still significant in terms of quantity (defined as 50+ records)
e) Anonymised information about patients or staff unless the anonymisation technique has been approved by the PHI's Data Guardian

Unless instructed otherwise, the home worker is responsible for ensuring that their home contents insurance cover extends to all provided equipment belonging to the PHI.

12.7 Security Procedures for home working

- The home worker's proposed working environment(s) must be considered and where necessary surveyed, and any perceived risks assessed to help inform consideration of home working options. The findings of this consideration or survey process and any associated risks must be documented, so that appropriate control measures may be reviewed.

- Where the proposed home working arrangements involve the use of personal or shared computing resources, it must be noted the risks of doing so may outweigh any operational advantage of home working. For all home working scenarios, consideration of risks must be made and must take account of the potential to:

    - accidentally breach confidentiality
    - disclose other sensitive data of the PHI to unauthorised individuals
    - lose or damage critical business data
    - damage the PHI infrastructure and e-services through spread of un-trapped malicious code such as viruses
    - create a hacking opportunity through an unauthorised internet access point
    - misuse data through uncontrolled use of removable media such as digital memory sticks and other media

- cause other operational or reputational damage

- When a home working agreement is possible the purpose, terms and conditions must be formally reviewed and agreed by the home worker. A reference copy of this agreement must be provided to the home worker. All such home working agreements must be reviewed periodically for their continued applicability

- Steps must then be taken to define, agree and implement the environmental security controls deemed necessary. The IT Security Manager must maintain records of all such assessments, surveys, related decisions, agreements and implementation plans

- It is the responsibility of the home worker to maintain their home working environment in conformance with the PHI policies and agreement permitting their home working. Where a home worker requires clarification or guidance they must consult the IT Support Manager

- The home worker must be made fully aware of their information governance responsibilities to the PHI. Training must be provided to home workers for any additional or special tools or functions that underpin the security of their home working, including provided access and log-on tokens. Such facilities and the training in their use are the responsibility of the IT Support Manager. This may for example include guidance on the deletion of cached information from internet browsers used to access web-based services

- Failure by staff to observe and maintain their home working agreement may result in their home working facility being withdrawn

- It is the responsibility of the IT Support Manager to ensure that the PHI infrastructure is maintained in a technically secure manner that would reasonably prevent a security breach arising from a home worker's location

- Once all necessary steps have been satisfied the home working arrangements agreed may be made operational. Please note that other IG codes of practice and good practice guidance for information governance security management, the use of data encryption tools and for the security of permitted removable media remain applicable and must be followed

- Audit spot checks must be considered by the PHI to ensure this home working policy is complied with and the agreement with the home worker must clearly specify that this may occur. Any compliance issues will be reported to the line managers concerned and may be handled through staff disciplinary processes or contractual arrangements

All incidents involving the use of home working facilities must be reported to the organisation's security manager immediately and in accordance with the organisations incident reporting procedures.

13. Data Retention

13.1 Minimum retention period

To comply with Data Protection Act ***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* it is necessary to establish what the minimum retention period should be for each type of data held.

De-identified data has no particular time limit and should be retained for as long as it is useful for research purposes.

13.2 Storage of Research Data

Researchers must determine the retention requirements for their research data and records on a project by project basis, or at least for clearly defined categories of projects, taking account of:

- The legal and regulatory framework for particular types of research;
- The terms and conditions imposed by external research sponsors;
- The commercial, political or ethical sensitivity of particular types of research, or any research for particular external sponsors.

Research data is inclusive of, but not limited to, all primary data sources, completed questionnaires, consent forms, audio and video recordings.

All non-anonymised personal data must be kept securely eg in a locked filing cabinet with restricted access or on a password protected computer.

As a general guide LJMU REC recommends that the following storage periods for all source data are maintained as a minimum.

Research Type	**Storage Period**
Undergraduate / Taught masters dissertations	1 month following conferment of the relevant award
MPhil / MRes dissertations	1 month following conferment of the relevant award
Doctoral level research (PhD, Prof Doc etc)	5 years after completion
Post-doctoral, staff research	5 years after completion

14. Data Removal Techniques

Many of the methods described in the following sections will be applicable to various different media types. It is recommended that specific removal methods are discussed with suitable vendors or contractors in line with the information provided in this guide.

A deletions log must be kept to show the Research project, dates of the data creation, number of records destroyed with method and dates of destruction.

14.1 Classification of Data Removal

There are two major data removal classifications that help determine the methods used as well as the possible costs involved. Data Clearing offers a fast method of data destruction using software applications but is only suitable for use on media which is to be redeployed in an environment of equivalent security controls to that of where the media was last used. Data Purging is a more thorough method of data destruction, and is used when media moves from an existing security zone to a new security zone. This new security zone may or may not be more secure than the current security measures in effect.

14.2 Clearing

If the disk drives/media will remain within the same environment in which they are currently situated (and existing security measures will continue to cover them), the most appropriate removal method is clearing.

Clearing involves simpler removal methods. As long as particular sections of data need removing and comprehensive data removal from the media is not required, then non-specialist staff or contractors may carry out clearing. Most ATA-type Hard Disk Drives manufactured after 2001 include the Secure Erase command within the drive firmware, which allows an administrator to quickly and effectively clear data from the drive. This process requires the installation of application software on the host system that can execute the Secure Erase command on the hard disk drive.

The Secure Erase command is also capable of overwriting reallocated disk sectors, where the drive has moved data due to hard errors. This provides an advantage over the use of data clearing software programs, which cannot erase bad disk sectors. For hard disk drives which do not offer Secure Erase support, software applications are available which perform sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs.

The US Center for Magnetic Recording Research (CMRR) has published further research and guidance on detailed processes for Data Destruction[1]. Their documentation supports the view that a single pass is sufficient to erase information from modern hard disk drives and that multiple on-track overwrites gave no additional erasure.

[1] http://cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf

Secure Erase has been approved by the U.S. National Institute for Standards and Technology (NIST), and is described in NIST document 800-88[2].

14.3 Purging

Purging is required when media moves from an existing security zone to a new security zone. This new zone may or may not be more secure than the current security measures in effect.

After removal of media from its current security context there must be sufficient care taken to ensure that data is irretrievable, even if specialised recovery methods are used (e.g. platter scanning or the use of electron microscopes).

For systems which support the Secure Erase command, the clearing process is technically equivalent to the purging process. Verification testing performed by CMRR shows that the erasure security is at the Purge level of NIST 800-88, because drives having the command also randomize user bits before storing on magnetic media.

The Full Disk Encryption Enhanced Secure Erase (FDE-SE) process proposes an enhancement to existing Secure Erase processes by changing the encryption key of the hard disk drive thus rendering any encrypted data on the drive inaccessible. It should be noted that FDE SE encryption is not yet tested for protection against advanced forensic analysis, and is presented here for information purposes. The use of a Secure Erase process following the use of FDE-SE would ensure the destruction of data for environments where this level of assurance is required.

14.4 Data Removal from Live Systems

There are various scenarios in which data may need removing from a system while still in operation, or reuse of the media is required for financial or policy reasons.

In these cases, organisations should make all possible efforts to remove the required data from the target media while not adversely affecting the performance of live systems or the long-term effectiveness of the media to perform the role required of it. In this case, the most common scenario would be to remove the data from hard disks or tape backup devices using processes built into applications or operating systems when a particular application no longer requires it.

14.5 Data Removal for Media Reuse

Often media such as hard disk drives are reused rather than being completely decommissioned. It is the reuse requirement, therefore, that should be the

[2] NIST Computer Security Resource Center, Special Publication 800-88: Guidelines for Media Sanitization, August 2006 (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

driving force behind the removal methods used (following the guidance above regarding clearing and purging).

In many infrastructure environments, hard disk reuse is common. A particular disk may be reused across many different individual machines or business uses. In this scenario, clearing is a sufficient method of ensuring data is non-recoverable. Keeping a log of all clearing processes (for each disk drive) provides an audit trail that records all the areas that the disk has been in use and, before reuse of the disk in a different area, the verification of data removal.

Best practice instructs that unless there is a compelling business reason to do so, media should not transfer between differing security contexts.

If media does require moving between security contexts, purging needs conducting in line with the guidance in this document to ensure that no data is retrievable, using any means.

Maintaining a log (including certificates of verification for each individual media device and information regarding the new use of the disk) is extremely useful as it ensures the media is traceable even after it has left its original security context.

14.6 Verification of Data Removal

If a specialist company or contractor has processed the media, there should be a procedure for verification of data removal, including the issuing of certificates.

If local staff have carried out the data removal then the process should be recorded with the verification results and stored with all other relevant documentation.

Tools that attempt to retrieve data from media which has undergone a data removal process can be extremely useful in verifying that complete data removal has taken place.

If any files or fragments of files are evident, then data removal has been unsuccessful. If so, repeat the process using a greater number of passes or consider using a different technique altogether.

15. Media Destruction Techniques Media Destruction

Media which is no longer required or has passed its effective reuse period should be destroyed according to the processes below, or passed to a specialist contractor for secure disposal. Organisations should ensure that where local data destruction and disposal is conducted, the methods within this document are followed and any waste products are disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE)

regulations[3]. Local contractors are available in most areas that are able to provide this service.

Where organisations choose to outsource the responsibility of data destruction and media disposal, the selected contractor should conform to the BS EN 15713:2009 standard. This sets out requirements for how sensitive information is collected, retained and transferred, the processes and standards for destruction, and the security measures for premises and personnel. Many of the techniques described for the destruction of media can involve dangerous substances or exposure to possibly toxic particulate matter, so can often require specially controlled environments and waste treatment processes.

15.1 Hard Disk Destruction

Due to the current costs of storage, large arrays of hard disks are utilised in preference to other backup methods, such as tape or optical storage. This is due to the speed and ease of retrieval and the added resilience of data when mirrored across many hard disk drives.

Degaussing is a simple method that permanently destroys all data and disables the hard disk drive. Degaussing uses a high-powered magnetic field that permanently destroys data on the disk platters. It also renders the drive hardware components inoperable, requiring manufacturer intervention to replace critical parts.

The recommended specification for data destruction is the SEAP 8100 standard used for classified government material. Equipment that complies with this standard assures complete data destruction.

Degaussing is generally safer for organisations to conduct than physical destruction processes and subject to the use of appropriate techniques the destruction of data is total and permanent. Degaussing equipment can be obtained by organisations and safely operated when following manufacturer instructions. Degaussed drives can then be disposed of as standard electronic waste which must be in accordance with the Waste Electrical and Electronic Equipment (WEEE) regulations. Local contractors are available in most areas that are able to provide this service.

Due to the component makeup of disk drives, only a specialist company in a secured and environmentally isolated location should undertake hard disk destruction. All casing materials must be removed and the disk platters disintegrated, to ensure the removal of all magnetic material. A disposal certificate must be obtained to document the destruction of hardware which contained sensitive data.

[3] http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

15.2 CD, DVD and BluRay Disc Destruction

The construction of plastic media such as CDs and DVDs makes them particularly vulnerable to damage if handled roughly. Most optical media consists of a plastic base with a laser sensitive substrate applied to one side. Optical media can be destroyed through the use of shredding machines that separate the disc into small pieces. All shredding machines must produce parts of no greater than 4mm x 32mm cross-cut to destroy sensitive data. Other optical media destruction systems are available, for example grinding machines which use a rotary handle attached to an abrasive pad to grind away the recording surface. These machines are very effective but expensive, and are therefore only likely to be cost-effective when disposing of large volumes of optical media. The discs should then be disposed through waste recycling processes.

Optical discs are made from Polycarbonate (No. 7 plastic) which often cannot be recycled using Local Council waste collection processes. Polycarbonate is a reusable material and chips can be reused to manufacture new items such as automotive parts, building materials, and safety equipment. Organisations should contact local plastic recycling companies in their area to recycle this material rather than sending it to landfill.

15.3 Solid State Device Destruction

Solid state devices include SSDs, Flash-based USB drives and memory storage cards for PDAs and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction of the device is required to ensure that any recovery of data is impossible. Disintegration and incineration are the most effective techniques for disposal of solid-state storage. Disintegration processes must break devices into pieces small enough to ensure that printed circuit boards and integrated circuit ‘chips’ are adequately destroyed. Guidance can be found in EN15713:2009 which specifies cutting sizes based on the size of the original device.[4]

Incineration processes will melt both the plastic casing and the internal circuitry of small components such as SD cards. This ensures that it is not possible to reuse or recover any aspect of the internal storage mechanism. Incineration processes should only be undertaken by specialist electronic waste disposal contractors.

Devices such as USB thumb drives should be physically destroyed using disintegration methods. In most cases a specialist contractor would be the most appropriate choice to destroy these devices, however organisations can undertake the disintegration process if required, where appropriate facilities exist. The outer casing must be removed and the internal circuitry must be broken into tiny fragments, including any integrated circuit ‘chips’ which can be cut or drilled to render them inoperable. Any plastic components should be recycled using local waste recycling facilities.

[4] http://www.bsia.co.uk/web_images//publications/form_204_id_en15713.pdf (see Tables 1 & 2, page 3)

If a solid state storage device has previously contained sensitive data, destruction should be carried out by a specialist contractor service and certificates obtained.

15.4 Magnetic Tape Backup

Magnetic tape formats vary significantly in their suitability for reuse and available clearing techniques. Some forms of magnetic tape can be degaussed and successfully reused as blank media. However some advanced tape formats rely on servo tracking data to record information on a blank tape, which is removed by the degaussing process and therefore makes this method unsuitable. Organisations should consult their hardware vendor for information on which system types will allow reuse of degaussed media. The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Various processes exist to disintegrate both the magnetic tape and the protective cartridge, with the possibility to recover and recycle the waste plastics produced.

Organisations should note that modern tape formats such as LTO Ultrium also contain EEPROM microchips which record potentially identifiable data such as tape library information, usage, and volume contents. Use of this storage mechanism is controlled by the backup management application. These types of tape cartridges must be disposed of by specialist computer waste disposal contractors, who conform to the BS EN 15713:2009 standard.

15.5 Paper Based

Traditionally, paper based disposal has consisted of simple vertical shredding. However this method is not suitable for sensitive or confidential information. The HMG Information Assurance Standard (IS5) requires the shredding of paper records be conducted using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm. This standard is in line with the requirements of BS EN 15713:2009 and is therefore recommended for the destruction of sensitive information.

Incineration processes may also be used to dispose of paper records and other types of printed media. A certificate of destruction from a specialist waste disposal contractor is required on completion.

16. Management of the Data Removal

It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring cleaning or destruction is correctly stored, organised and properly accounted for. The use of a data removal and destruction process also helps to achieve successful audit results by demonstrating repeatable steps and records of media which was processed.

It is recommended that a log of all media is kept that may contain sensitive information. This should detail the specification of the media and its effective end of use date.

Use of inventory tracking software may be helpful in limiting the administration overhead in larger organisations. Tracking of hard disk serial numbers should be used as a minimum control for individual component tracking where other methods are not available.

The log should also contain a section for destruction or removal certificates; these provide evidence guaranteeing the destruction or sanitisation of the media by the nominated waste disposal contractor and the date on which the destruction occurred.

17. Information Risk Assessment

17.1 **Objective**

To identify and assess Information risks to Business as Usual within the PHI, enabling actions to be taken to minimise the effect.

17.2 Methodology

The method of information security risk assessment applied throughout the PHI is the Australia/New Zealand model of assessing risk.

A risk is defined by the Australia/New Zealand Standard for Risk Management (*AS/NZS 4360:2004*) as

> *"…the possibility of something happening that impacts on your objectives. It is the chance to either make a gain or a loss. It is measured in terms of likelihood and consequence."*

17.3 Identify the risks

- The assets within the scope of each risk assessment are identified and listed in line with the business requirements of the PHI

- When new information assets are acquired, or existing assets in any way change, those assets are added to the inventory of the PHI and are treated in line with the requirements below

- **Threats** to each of those assets shall be identified under the headings of threats to availability, confidentiality and integrity and are documented in the asset risk log

- **Vulnerabilities** that might be exploited by each of these threats are identified and documented with each risk assessment

- Where new vulnerabilities or weaknesses are identified, the risk log shall be updated and, where appropriate, the risk assessment procedure set out here shall be repeated and any changed controls implemented

- The effect that losses of availability, confidentiality and integrity might have on the assets themselves (i.e. what is the actual harm to the asset itself that might occur?) are identified and documented

17.4 Assess the risks

- **Impacts** – the business harm - that might result from the loss of availability, confidentiality or integrity, for each of these assets, is assessed

- The realistic likelihood that each of these failures might occur is assessed

- The risk levels are assessed

- A decision is made, for each of the risks, as to whether it is acceptable or if it must be controlled in line with criteria established

17.5 Identify and evaluate options for the treatment of risks

- For each of the risks, identify the possible options for treating it in line with the decision made above

- For each of the risks, document which treatment action (accept, reject, transfer or control) is going to be taken and document in the PHI risk treatment plan the reasons for each choice

17.6 Select control objectives and controls for treatment of the risks.

- Appropriate control objectives are selected from Annex A of BS7799-2:2005/ISO 27001 and the reasons for the selections are documented in a detailed working document in the light of the conclusions to the risk assessment and risk treatment processes

- These control objectives and controls are then summarized into the PHI's information security management system

- The DPA Compliance Group is the owner of this document section and is responsible for ensuring that its procedures are reviewed and followed in line with the requirements of the PHI and that Information Risks are entered into the Risk Register as appropriate

18. Incident reporting

18.1 Objective

To ensure that any observed incident that could compromise information confidentiality or security is reported quickly and correctly.
The PHI recognises that threats to the information services it provides can compromise patient confidentiality as well as security of information, equipment, patients and staff. This section defines where to find the procedures to be followed for the recording of information incidents, their

monitoring, review and mitigation of future risks by changes to actions and operational procedures.

18.2 Scope

Confidentiality of PID is required as defined in the PHI's Confidentiality Code of Conduct.

There are several ways in which patient confidentiality may be breached such as theft, break-ins and poor disposal of confidential waste. All breaches must be investigated and reported accordingly. The mechanisms for handling security incidents where patient confidentiality has been or may have been breached are defined in the PHI's Information Incident Reporting Procedure.

The majority of IM&T security breaches are innocent and unintentional such as the user not 'logging out' at the end of the day. However 'near misses', where no actual harm results from the incident, should still be reported and analysed to look for possible ways of preventing an actual incident occurring in the future.

18.3 Definitions

An Information security incident is defined as any event that has resulted or could result in:

- the disclosure of confidential information to any unauthorised individual
- the integrity of a system or data being put at risk
- the availability of a system or information being put at risk

An adverse impact can be defined for example as:

- threat to personal safety or privacy
- legal obligation or penalty
- financial loss
- disruption of PHI business
- an embarrassment to the PHI

18.4 Types of Security Incidents

The types of security incidents likely to affect patient confidentiality are variable. Information security incidents may take many forms including the following:

- Theft of equipment holding confidential information – PCs, laptops. Smart-phones, dicta-phones, case-notes, etc.
- Unauthorised access to a building or areas containing unsecured confidential information
- Access to patient records by an authorised user who has no work requirement to access the records
- Authorised access which is misused (staff)
- Electronic access (hacking) and viruses

- Misuse of equipment such as faxes, text messages on mobiles and e-mails
- Inadequate disposal of confidential material (paper, PC hard drive, disks/tapes, etc)
- Car theft / break-ins to staff carrying patient information
- Unauthorised access to records away from premises (e.g. laptops and notes when travelling between clinics to home-visits etc)
- Complaint by a patient, or a member of the public, that confidentiality has been breached
- Careless talk. "Loose lips sink ships."

The Information Security Manager or Department Risk Manager will report Information incidents to the IT Support team and the DPA Compliance Group and, via this channel, to the Director.

19. Roles and Responsibilities

19.1 Director

The Director has overall responsibility for DPA Compliance in the PHI. This responsibility is discharged through the Deputy Director, who has lead responsibility for DPA Compliance in the PHI.

19.2 SIRO

The PHI Senior Information Risk Owner (SIRO) is responsible for understanding how the strategic business goals of the PHI may be impacted by information risks and for the ongoing development and day-to-day management of the PHI's Risk Management Programme for information privacy and security.

The SIRO will review and agree action in respect of identified information risks, ensure that the PHI's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

The SIRO will provide a focal point for the resolution and/or discussion of information risk issues and ensure the Board is adequately briefed on information risks. The SIRO also:

- Should monitor the progress of the DPA Compliance action plan and report progress to the PHI Board

- Provides the escalation route for dealing with any issues promoting risk to action plan progress, through discussion with other directorate heads

19.3 Data Guardian

The PHI's Data Guardian has a particular responsibility for reflecting

patients' interests regarding the use of patient identifiable information and is responsible for ensuring patient identifiable information is stored, used and shared in an appropriate and secure manner.

19.4 IT Support and Security Manager

19.4.1 IT Support aspects

- To ensure appropriate notification in compliance with the Data Protection Act 1998 is maintained for the PHI's stored information.

- Is responsible for dealing with enquiries about DPA Compliance issues, and facilitating Subject Access requests

- Is responsible for advising and training staff on their DPA Compliance responsibilities

- Is responsible for advising on actual or potential breaches of confidentiality, and recommending remedial action

- Is responsible for ensuring The PHI has procedures in place to comply with relevant Department of Health best practice guidance such as Confidentiality code of practice and Records Management code of practice

- Is responsible for liaising with external organisations on DPA Compliance matters

- Is responsible for the development and implementation of Information sharing protocols

- Is responsible for approving user access profile templates

19.4.2 IT Security Management aspects

- Responsible, on behalf of the Director, for implementing, monitoring, documenting and communicating information security within the PHI, in compliance with UK legislation and national policy and guidance

- Must monitor and report to the Director (via the DPA Compliance Group) the state of information security within The PHI

- Must have ready access to the Data Guardian for guidance on confidentiality policy

- Must liaise with the DPA Compliance Group regarding the information security input to the DPA Compliance agenda

- Must liaise with relevant senior, line and system managers over information security

- Must liaise with Senior Management regarding information security at the operational level

- Must liaise with the SHA Registration Authority Manager where changes to national / local security policy affect registration activities

- Must ensure that this Information Security Management System is implemented and followed throughout The PHI

- Must ensure that relevant staff are aware of their security responsibilities and that security awareness training is provided for all staff

- Must ensure that IT system users know how to report any security breaches, incidents, malfunctions and suspected system weaknesses and threats

- Must monitor for actual or potential information security breaches within the PHI

It is essential that the manager, or managers, responsible for DPA Compliance and security management must work in close association with the manager or managers responsible for freedom of information, data protection, patient confidentiality and other DPA Compliance work areas.

19.5 Line Managers

- Should ensure all current and future staff are instructed in their security and IG responsibilities

- Are responsible for ensuring that the policy and supporting standards and guidelines are built into local processes and that there is on-going compliance

- Must ensure that the leaver process is carried out promptly and correctly when staff leave

- Must comply with Standing Orders and policy on potential personal conflicts of interest

19.6 All Staff

- Each employed, contracted and voluntary staff member is personally responsible for ensuring that no breaches of computer security or information confidentiality result from their actions

- Must comply with the PHI's relevant security and confidentiality policies and procedures

20. Internal Audit

The DPA Compliance Group will monitor the implementation of this, and any subsequent revisions. An annual internal audit covering all aspects of the DPA Compliance Group will be carried out .

21. Management Review of the ISMS Framework

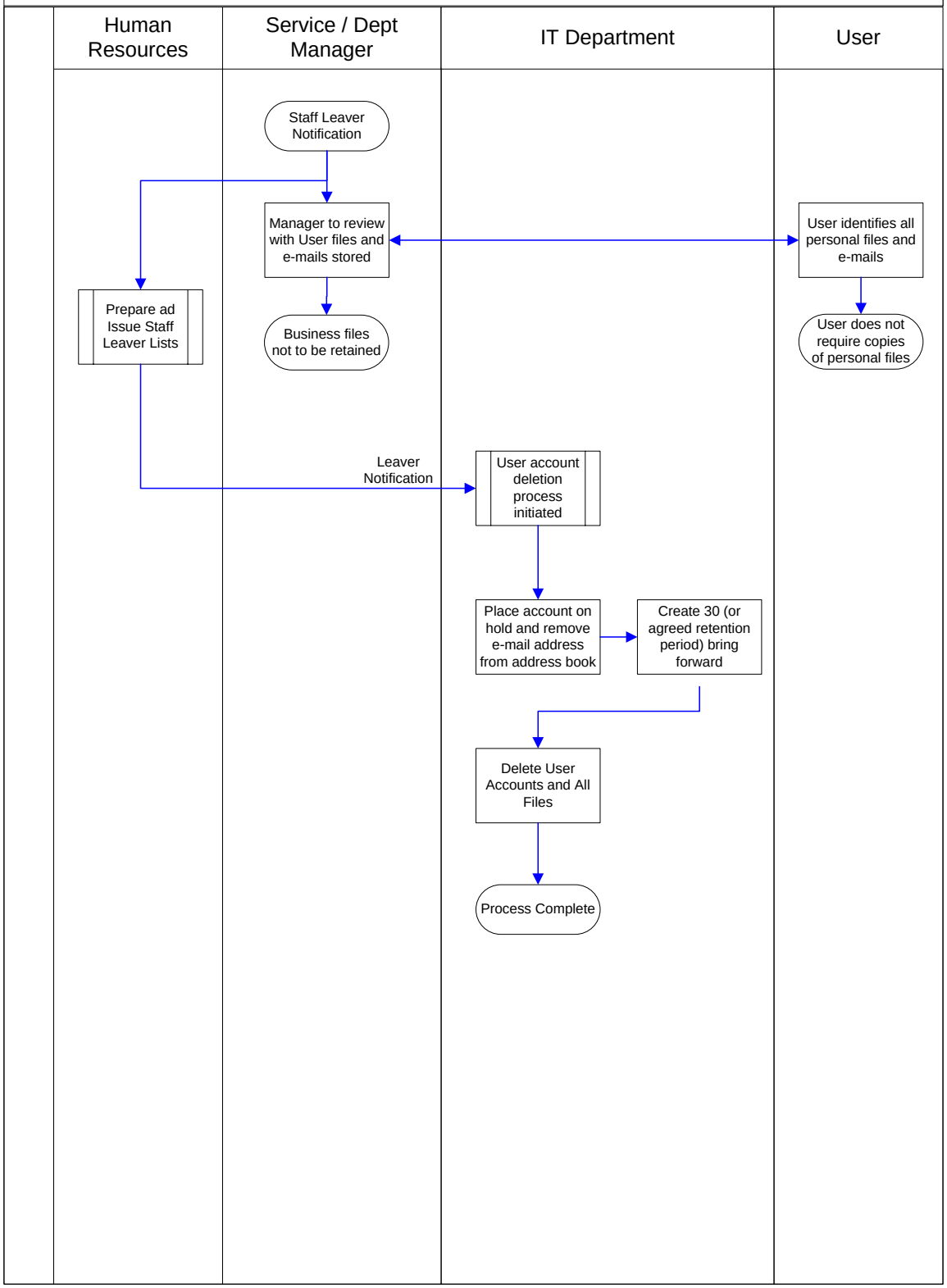
This process must be reviewed by Management at planned intervals (at least once a year) to ensure continuing suitability, adequacy and effectiveness. Objectives and opportunities for improvement to the procedures that support the ISMS shall also be reviewed.

This document must also be subject to review when any of the following conditions are met:

- The adoption of the system highlights errors or omissions in its content
- Where other policies/strategies/guidance issued by the PHI conflict with the information contained herein
- Where the procedural or guidance framework evolves/changes such that revision would bring about improvement
- 1 year elapses after approval of the current version

Appendix 1 Network files and E-Mail Accounts – Deletion

Fig 1 - Deleting User Access And E-Mail Accounts - Routine Process



Appendix 2 Network files and E-Mail Accounts – Retention

Fig 2 - Deleting User Access And E-Mail Accounts