The National Confidential Inquiry into Suicide and Safety in Mental Health

Information Security and Management Policy

Standards and Procedures

Version 17

Document Name:	Information Security and Management Policy - Standards and Procedures		
Date:	January 2021	Release:	Final
Originated July 2003 by:	Jo Robinson, Senior Project Manager Kirsten Windfuhr, Project Manager		
Author of current version:	**Huma Daud** (IT Officer for the National Confidential Inquiry into Suicide and Safety in Mental Health) **Pauline Turnbull** (Project Director for the National Confidential Inquiry into Suicide and Safety in Mental Health) **Rebecca Lowe** (Information Governance Officer)		
Document Number:	ISMP/17		
Circulation	Master electronic copy is located in G:\INQUIRY_info Security\NCI Security Policy v17_JUL2023 One hard copy held in the Main NCISH Office (including all appendices). One hard copy of Appendix G BackupProcedure_JUL2023_v17 FINAL.doc and Appendix H Business Continuity Guide_JUL2023_v17 FINAL.doc held in the Main NCISH Office in the Server Cabinet.		
Authorised by:	**Professor Sir Louis Appleby** (Director – Centre for Mental Health and Safety in which NCISH is based)		
	Signature:		
	Date:		

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Next Revision
July 2010	October 2008	Listed independently of this document. Held by A Williams, Deputy Project Manager of the National Confidential Inquiry into Suicide and Homicide by People with Mental Illness	July 2011
June 2011	July 2010	Listed independently of this document. Held by A Williams, Deputy Project Manager of the National Confidential Inquiry into Suicide and Homicide by People with Mental Illness	June 2012
December 2012/ January2013	June 2011	Listed in: G:\INQUIRY_info Security\NCI Security Policy v10_July2012\ISMP MASTER FILESv10July2012\ISMP_V10_Details of Amendments.doc	Summer 2013 as part of IG Toolkit completion – revision occurred in lead up to IGT first submission
September 2014	Summer 2013 – revision actually occurred in lead up to IGT first submission 06/01/14	Listed in: G:\INQUIRY_info Security\NCI Security Policy v11_Aug2014	Summer 2015 in advance of next IGT submission
December 2015	September 2014	Listed in: G:\INQUIRY_info Security\NCI Security Policy v12_DEC2015\ISMP_V12_Details of Amendments_Dec2015.doc	December 2016
January 2017	December 2016	Listed in: G:\INQUIRY_info Security\NCI Security Policy v13_JAN2017\ISMP_V13_Details of Amendments_Jan2017.doc	December 2017
January 2018	January 2017	Listed in: G:\INQUIRY_info Security\NCI Security Policy v14_JAN2018\ISMP_V14_Details of Amendments_Jan2018.doc	January 2019
January 2019	January 2018	Listed in: G:\INQUIRY_info Security\NCI Security Policy v15_JAN2019\ISMP_V15_Details of Amendments_Jan2019.doc	January 2020
January 2021	January 2019	Listed in: G:\INQUIRY_info Security\NCI Security Policy v16_JAN2021\ISMP_V16_Details of Amendments_Jan2021.doc	January 2022
July 2023	January 2021	Listed in: G:\INQUIRY_info Security\NCI Security Policy v17_JUL2023\ISMP_V17_Details of Amendments_JUL2023.doc	July 2023

CONTENTS

1. Introduction

1.1. Introduction

1.1.1. This document was initially developed in 2003 in support of the application by the National Confidential Inquiry into Suicide and Safety in Mental Health (also known as NCISH), formerly known as The National Confidential Inquiry into Suicide and Homicide by People with Mental Illness (formerly also known as the Inquiry) to hold patient identifiable information under the provisions of Section 60 of the Health and Social Care Act (2001). Since then, the document has been reviewed regularly in light of evolving guidance on information governance, data protection and confidentiality. In this version, current legislation, NHS guidelines and codes of good practice, the requirements of the NHS Data Security and Protection Toolkit and the University of Manchester's own guidance, have been consulted (see Section 25: References).

1.2. The need for an Information Security and Management Policy (ISMP)

1.2.1. Data stored in computer and other information systems are valuable assets. Many work processes are electronically controlled, and large amounts of information are stored in digital form, electronically processed and transferred on local and public networks. Many tasks performed within both NCISH and the University are difficult or impossible without the use of IT. Consequently, this organisation is reliant on the correct functioning of our IT assets and their proper use.

1.2.2. The potential damage that could result from malfunction or failure of IT varies from a minor inconvenience to the entire department being unable to work, resulting in time and financial losses. Breaches of confidentiality could result in legal action; loss of data integrity and loss of data authenticity. Malfunction / failure of IT and breaches of confidentiality would also have serious consequences for NCISH's reputation as a leading research centre in mental health care.

1.3. Focus of the ISMP

1.3.1. The primary focus of the ISMP is on the security requirements necessary to safely carry out NCISH's main role, that is, the receipt and processing of sensitive, person identifiable information (general population data) from central government sources, and the acquisition of medical history for individuals receiving mental health care (patient data). It specifies the access to, and the maintenance and control of, the Centre for Mental Health and Safety's independent server and networked computers. However, as NCISH is part of the University, the ISMP also reiterates staff responsibilities when using university networked information systems.

1.3.2. Key issues addressed by the ISMP are:

- **Confidentiality** - data/information access is confined to those with specified authority to view the data.
- **Integrity -** all system assets are operating correctly according to specification, and the information is accurate and complete in storage and transport.
- **Availability** - information is available to those who are authorised to have it, when and where they should have it. Adequate controls contribute to the continuous availability of systems.
- **Accountability** – all staff are aware of their responsibilities towards security and confidentiality and are held accountable for their actions.

1.3.3. The University also has legal obligations to maintain security and confidentially notably under the General Data Protection Regulation (GDPR), applicable from 25 May 2018, the Human Rights Act 1998, the Computer Misuse Act 1990 and the Copyright, Designs and Patents Act 1988.

1.4. Scope of the ISMP

1.4.1. The ISMP applies to all NCISH equipment and information whether on site or off-site.

1.4.2. This policy aims to ensure that:

- Information will be protected and controlled against unauthorised access or misuse.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Information security training will be provided to all staff.
- Confidentiality statements will be issued and signed by all personnel.
- Physical, logical, environmental and communications security will be maintained.
- Operational procedures and responsibilities will be maintained.
- Line managers understand their responsibility for the implementation of the policy within their area, and for adherence to it by their staff.
- All staff are aware that it is their responsibility to adhere to the policy.
- All breaches of information security will be reported and investigated through the appropriate management channel.

In addition:

- Standards and procedures will be produced and measures implemented to support the policy.
- The ISMP will govern standards, procedures and setup of the CMHS (see Appendix A Glossary of Terms) network as stated in the Appendix I System Level Security Policy (SLSP).
- Deliberate infringement of the security policy may result in immediate disciplinary action or criminal prosecution.
- The IS&M Team (See Appendix A, Glossary of Terms) along with the NCISH Management Team have direct responsibility for maintaining the policy and providing guidance and advice on its implementation.
- The Director of NCISH has overall responsibility for the Information Security and Confidentiality Policy; day to day operational responsibility lies with the Project Director and Information Governance Officer.

1.4.3. Information is defined as (but not limited to):

- Electronic data including facsimiles.

- Paper based data.
- CCTV and videos.
- Verbal and telephone conversations.
- Photography and other images.
- Recorded sounds.

1.5. Potential threats

1.5.1. The policy has been designed to address the following risks:

- Fraud - altering data or information for private gain or benefit, altering or misusing programs, destroying/suppressing/misappropriating NCISH or University information or computer output.
- Virus - introducing viruses, or other malicious software to University computers and systems.
- Theft – of data, software and hardware.
- Use of unlicensed software - using illegal copies of software.
- Private work - unauthorised use of the University's computing facilities or materials for private gain or benefit.
- Hacking – deliberately gaining unauthorised access to a computer system.
- Sabotage – causing deliberate damage to data, software, processes or equipment.
- Misuse of personal data – unofficial access to data or 'browsing' through computer records and breaches of the Data Protection legislation.
- Introduction of inappropriate material - access to or processing of inappropriate material.

1.5.2. It is important to ensure that the security of an information system must be reasonable and practical.

1.5.3. Human attitudes are fundamental to good security. Managers, users and operators must be aware of the reasons for taking security issues seriously.

1.5.4. Deliberate misuse of either NCISH's or University's information, computer or communications systems by an employee may result in disciplinary action. More serious misuse, for example, sabotage, theft, breach of confidentiality, accessing pornography, hacking, introducing viruses or causing harassment to others may result in the dismissal of the employee.

2. Management of Security and Confidentiality

2.1. Objective

2.1.1. To establish the management structure for information systems security within NCISH.

2.2. Organisation management

2.2.1. The IS&M Team (See Appendix A, Glossary of Terms) will have organisational security management responsibilities for:

- Ensuring that the ISMP is implemented throughout NCISH.
- Developing and enforcing detailed procedures to maintain security.
- Ensuring compliance with relevant legislation.
- Ensuring that NCISH personnel are aware of their responsibilities and accountability for ensuring information security and confidentiality.
- Monitoring for actual or potential breaches of the ISMP.

2.2.2. Detailed responsibility for maintaining and reviewing protocols for secure data processing and management, and for infrastructure integrity and security will be delegated to the NCISH Project Director, Information Governance Officer and Research IT.

2.3. Auditors

2.3.1. The ISMP will be subject to review by NCISH's IS&M Team, (see Appendix A, Glossary of Terms), the recommendations from which will be considered carefully by the Senior Management Team and implemented as appropriate/required. The ISMP will be made available for scrutiny by NCISH's funders and authorities that supply data (e.g. the Office for National Statistics) or have responsibility for maintaining information governance standards (e.g. NHS Health Research Authority Confidentiality Advisory Group, NHS Digital) as appropriate.

2.4. Authorisation process for new IT facilities

2.4.1. The IS&M Team or the Senior Management Team (Appendix A, Glossary of Terms) must approve major new IT systems and services. IT equipment must be for a defined business purpose and provide an adequate level of security protection. Additionally, it must not adversely affect the security of the existing infrastructure.

2.4.2. Three levels of authorisation are required:

- **Corporate approval –**.For developments to CMHS systems (Appendix A Glossary of Terms), approval will primarily rest with NCISH's Senior Management Team in consultation with users (and user managers) of the proposed system and University IT advisors (see 'Technical approval' below)
- **Technical approval –** See 9.4.1. Purchase of new IT equipment must be made in consultation with Research IT. The University currently has an agreement with a supplier to provide PCs/Laptops to a standard specification. Purchase of new IT equipment must be made in consultation with Research IT /IT Service Desk – see Appendix A, Glossary of Terms.
- **Security approval –** The IS&M Team should ensure the system and its implementation conforms to the Information Security and Management Policy.

3. Security Responsibilities

3.1. Objective

3.1.1. To ensure that NCISH's staff are aware of physical security risks, (e.g. unauthorised access to NCISH offices), NCISH and University information systems security risks and their responsibilities to minimise the threats.

3.1.2. To ensure that all staff are aware of the implications of non-compliance with the policy.

3.2. Management responsibilities

3.2.1. Security is ultimately the responsibility of all staff at all levels in NCISH. Managers should ensure that adequate attention and resources are applied to security issues in the development and operation of both NCISH and University information systems. To ensure that the security of NCISH systems is managed in an integrated fashion throughout the organisation, the Senior Management Team will allocate overall day-to-day responsibility for security to the Project Director, (reporting to the Director) whose authority for security issues should span all projects within NCISH.

3.2.2. All staff that design, develop, operate, maintain or use information systems have responsibility for the security of these systems. Day to day operational security of NCISH information systems will be the responsibility of Research IT. Research IT will also liaise with central University IT teams in the event of the inappropriate use of University information systems.

3.2.3. The IS&M Team should:

- Ensure that all current and future staff are instructed in their data protection, confidentiality and computer security responsibilities at induction and at the time of signing the Confidential Disclosure Agreement at the start and at the end of employment. Individuals must be made fully aware of the possibility of disciplinary or legal proceedings that may result if a breach of confidentiality occurs.
- Ensure that all their staff using computer systems/media are trained in their use.
- Ensure that no unauthorised staff are allowed to access any of NCISH's computers, communications and information systems as such access could compromise data integrity.
- Determine which individuals are to be given authority to access specific computer systems. The level of access to specific systems should be on a job function need, independent of status. Access levels should be clearly defined and documented. See Appendix B, Shared Folders, Active Directory User Groups and Users Group Membership.
- Implement procedures to minimise NCISH's exposure to fraud/theft/disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas.
- Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability.
- Ensure that appropriate security measures shall be taken against unauthorised access, alteration, disclosure or destruction of personal information, whether accidentally or intentionally.

- Ensure that the Research IT are advised immediately about staff changes affecting computer access so that passwords may be withdrawn/deleted and access to corridor withdrawn (see 3.3.4).

- Ensure the various assets and security processes associated with each individual system are identified and clearly defined.

- Ensure that where work is, or has the potential to be, critical to the organisation, more than one person can undertake this work. Such critical tasks must also be fully documented to reduce the risk of compromise of service. See Appendix B, Shared Folders, Active Directory User Groups and Users Group Membership (Terminology section) for details of staff that are authorised to access the CMHS's primary server in the absence of Research IT.

3.3. Termination procedures

3.3.1. The timing of the following requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

3.3.2. Prior to an employee leaving, or to a change of duties, line managers should ensure that:

- Passwords are removed or changed as appropriate.

- Relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists.

- Supervisors' passwords allocated to the individual should be removed and consideration given to changing higher-level passwords, to which they have access.

- Staff responsible for controlling access to secure or restricted areas, are informed of the termination, and are instructed not to allow admission in future without authorisation (see 3.3.4).

- It may be appropriate to assign staff to non-sensitive tasks whilst working out their notice. In this case access should be changed to suit the situation.

- University and NCISH property including data or information is returned and assurance given that no information has been copied or retained.

- A 'leaving declaration' is signed by the individual that states that they do not hold on any personal laptop, other personal data storage device or in paper format any data for which NCISH is either an authorised data processor or data controller (see also 3.4.12).

3.3.3. Particular attention should be paid to the return of items that may allow future access. These include personal identification devices, cards, keys, passes, manuals and documents.

3.3.4. When staff leave NCISH, in the first instance, the IG Officer must be informed so that swipe card access to the corridor can be removed. In the absence of the IG Officer, the University Access Control Manager should be informed so that they can remove swipe card access to the corridor, see Appendix A, Glossary of Terms.

3.4. Staff responsibilities

3.4.1. All staff must adhere to the ISMP procedures and standards. Failure to do so may result in disciplinary action up to and including dismissal.

3.4.2. Staff must not transfer personal information from University computer systems, (e.g. email) to any other device that is not registered with NCISH including but not limited to CD's, portable hard drives, laptop, USB pens/sticks or any other portable storage media or device. Where data must be transferred onto a portable device in order to transfer it to NCISH systems, the device must be password protected and/or encrypted and also be registered with NCISH. See the NHS Digital general guidance at https://digital.nhs.uk/services/data-access-request-service-dars/data-access-request-service-dars-process/data-access-request-service-dars-guidance-notes-on-security.

3.4.3. Each employee is personally responsible for ensuring that no breaches of confidentiality or system security result from their actions.

3.4.4. Under no circumstances can staff sell or otherwise disclose NCISH or University information for personal profit or gain.

3.4.5. Each employee must ensure that any person receiving information is authorised to receive it. Where there are doubts checks should be made to ascertain the identity of the recipient prior to disclosure.

3.4.6. **Employees must report any breaches of security or security incidents to the IS&M Team promptly via their line manager (see also Section 20 and Appendix E Asset Information Loss)**.

3.4.7. Each employee should declare any potential conflicts of business interest as required by the University's regulations.

3.4.8. Sensitive data must be cleared from desks and computer screens blanked when workstations are unmanned; especially when the user is absent for a long period or has ceased work. This should be automated where possible.

3.4.9. Confidential patient-identifiable information must not be saved to the user's hard drive. If it is necessary to save this information e.g. CMHS network is unavailable due to some fault, NCISH approved media must be used which is password protected and/or encrypted and then stored in a safe – see Section 16 on Portable Electronic Devices. When there is no longer a requirement for the information to be on the media, it should be electronically shredded using appropriate software.

3.4.10. In case of theft or unauthorised access, staff should ensure that person-identifiable data is not kept on their PCs.

3.4.11. Staff who leave NCISH must ensure that all loaned IT equipment is returned to NCISH prior to leaving.

3.4.12. Staff who leave NCISH must ensure that all information is returned to NCISH and additional copies destroyed.

3.4.13. Any member of staff attempting to, or gaining illegal unauthorised access, to the University's or NCISH's systems will be subject to disciplinary action. There may be a circumstance in which immediate dismissal is appropriate.

3.4.14. Information or data destined for a specific individual, department or organisation must not be deliberately prevented from reaching its intended destination; further, unauthorised individuals or organisations must not modify information or data contents.

3.4.15. Due to COVID-19, many NCISH staff will be working from home instead of within the NCISH offices. In order to do this responsibly, staff are not permitted to remove any identifiable data from the NCISH network and are only able to work on anonymised datasets. Staff who are required to access identifiable data must attend the NCISH offices in order to do so, in line with our data management protocols.

3.5. Audit of information output

3.5.1. Any member of staff who sends patient or staff-identifiable information off-site should maintain a record that holds details of:

- The type of data sent.
- The recipient.
- The date of despatch.

Confirmation of receipt can be obtained from recipients by:

- Sending information via recorded deliveries.
- Obtaining confirmation in writing, e.g., a return slip on a covering letter.

3.5.2. Delivery of the information should be by secure means. Externally this could mean electronically (via NHS N3 network), using a trusted carrier, e.g. Royal Mail Special Delivery or a reputable Courier, whilst deliveries which are in and around the local site, should be by special and direct service (i.e., sensitive items should not be left unattended by messengers with other duties to perform). See also Appendix I, System Level Security Policy, section heading Operational Processes.

3.5.3. It should be established that all recipients of data or information are registered with and comply with the General Data Protection Regulation and that they are taking adequate measures to safeguard the confidentiality of all patient data received.

Registration can be verified by checking on the Information Commissioners website: https://ico.org.uk.

3.6. Research IT Team

3.6.1. Research IT – see Appendix A, Glossary of Terms - will take day to day responsibility for the security of the systems and the data therein. Research IT are the first point of contact for NCISH staff experiencing difficulties with the CMHS private network and/or if problems with the University's systems are encountered, including e-mail and Internet access. If Research IT are unable to assist with problems with the University's systems, this will be logged as a call with the University IT helpdesk.

3.6.2. Research IT and the IG Officer should ensure that all NCISH and university systems are operated in accordance with the ISMP.

3.6.3. Research IT will undertake system specific compliance assessments. This would be in the form of periodic audits, see section 8.3.1. They will also plan and monitor effective solutions to areas of weakness with regard to the ISMP.

3.6.4. Research IT will ensure that all staff are aware of the University's regulations and policies regarding use of email and internet access. The policies may be viewed at https://www.itservices.manchester.ac.uk/aboutus/policy/.

3.6.5. The master copy of the ISMP is the electronic version stored on the CMHS primary server G:\INQUIRY_info Security\NCI Security Policy v17_JUL2023\ NCI Info Security and Management Policy_JUL2023_v17_FINAL.doc. One paper copy is stored in the main NCISH office and has a "FINAL" watermark running through it. Paper copies of Appendices G and H only (Backup Procedure and Business Continuity Guide respectively) are also stored separately in the main NCISH office in the Server cabinet. In the event of being unable to access the server, the IS&M Team have access to a copy of the ISMP stored on a shared University drive, 3.

3.6.6. It is important to ensure that a copy of the documents outlining the procedures necessary for the secure operation of the system is to hand. It must be available to all users and they must comply with the requirements.

3.6.7. The job description for Research IT will include specific reference to the security role and responsibility of the post.

3.6.8. The CMHS network should have at least 2 individuals within NCISH with the expertise to administer the day-to-day running of the system. See Appendix B, Shared Folders, Active Directory User Groups and Users Group Membership (Terminology section) for details of NCISH staff that have authorisation to access the CMHS's primary server in the absence of Research IT.

3.6.9. Research IT will be responsible to the IS&M Team for the continuance of system security.

3.6.10. All systems should include validation processes at data input to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity.

3.6.11. Systems should report all errors together with a helpful reason for the rejection to facilitate correction.

3.6.12. All systems will incorporate internal validation processes and audit trails to detect and record problems with processing/data integrity.

3.6.13. The use of "mandatory fields" should be applied where necessary.

3.6.14. Error reports will be produced and will be actioned regularly.

3.7. System users – data quality

3.7.1. Data quality/accuracy is the direct responsibility of the person inputting the data, supported by their line manager.

3.7.2. Error correction should be done at the source of input as soon as it is detected. Such correction is increasingly important as systems are linked and errors can be transmitted between systems.

3.7.3. Any loss or corruption of data should be reported to Research IT immediately.

3.8. Contracted staff

3.8.1. Contracted staff, at any level, should be subject to the same disciplines relating to security issues as permanent members of staff.

3.9. System developers

3.9.1. The development of new information systems must include consideration of security issues. Any additional costs may be balanced by avoiding a design option which may later have to be abandoned on security grounds or may need disproportionate effort to make it secure.

3.9.2. Protocols must be written when new systems are developed in-house.

3.10. Intellectual property rights

3.10.1. Intellectual property rights can be defined as products of creativity; innovation or research and development. Such property can be given legal recognition of ownership as intellectual property rights through:

- Patents.
- Copyright.
- Design rights.
- Trademarks.
- Know-how.

Intellectual property related to copyright and database design are most applicable to the work of NCISH.

3.10.2. The University recognises that, from time to time during the normal course of employment, a member of staff may generate intellectual property. Such intellectual property could have commercial or other value. Intellectual property created in the course of or pursuant to commissioned research or other agreement with an outside body (in NCISH's case – with the Healthcare Quality Improvement Partnership (HQIP)) will be determined according to the terms the contract between the University and the commissioners. The University of Manchester's IP Policy is available in detail on the University's website.

3.11. Copyrighted material

3.11.1. Copyright of material produced by University employees would normally remain the property of the University, the research funders, or the data providers as appropriate. However, the University usually grants a free licence to the copyright of any work to be published in a recognised scientific, technical, professional or management journal or book to the author. The University will not normally take any action to diminish or remove the moral rights of University employees in respect of copyright (i.e. the right to be named as author). The University will not grant such licence to the copyright of materials created by a member of staff during the course of and related to their employment. This includes (but is not limited to):

- Course or training materials.
- Software programmes.
- Any designs, specifications or other works, which may be necessary to protect rights in commercially exploitable intellectual property.

3.12. Purchased systems

3.12.1. New systems that are procured externally must be carefully examined from a security and suitability viewpoint and any additional cost should be considered part of the price for improving security as a whole.

4. Confidentiality of Information

4.1. The Common Law Duty of Confidentiality

4.1.1. It is a general principle of the Common Law Duty of Confidentiality that information given or obtained for one purpose should not be used for a different purpose before it is effectively anonymised, without the express or implied authorisation of the provider of the information. See the Records Management Code of Practice for Health and Social Care 2021, Section 25 References. Therefore under the Common Law Duty of Confidentiality personal health information is strictly confidential.

4.1.2. Personal health information should not be disclosed without the patient's consent, except in exceptional circumstances e.g., to safeguard the individual, or others, or is in the public interest or there is a legal duty to do so (i.e., court order).

4.1.3. Patients should be made aware of the circumstances in which information disclosure must take place, e.g. between medical teams in order to deliver appropriate medical care, and that there may be other legitimate purposes for which their information might be shared, e.g. clinical audits.

4.1.4. Personal health information must be anonymised wherever possible, unless there is a need for the identity of the patient (or another individual) to be disclosed.

4.1.5. Everyone involved in the handling of health information in the NHS has a legal duty, reinforced by their contract of employment (or equivalent formal relationship), of confidentiality towards patients and towards the NHS bodies to which they are answerable.

4.1.6. Doctors and other health professionals have an ethical duty, by virtue of their profession, of confidence towards their patients. NHS bodies owe a similar duty of confidence towards both patients and to the health professionals who work within the NHS, to preserve those ethical standards of confidentiality to which the professions adhere.

4.1.7. If there are any doubts regarding appropriate disclosure to others, staff must seek advice from the Project Director who will consult with as appropriate, the Senior Management Team, Information Governance Office (Contact: 0161 306 6000). The advice of NCISH's lead mental health trust Caldicott Guardian (Greater Manchester Mental Health NHS Foundation Trust) may also be sought depending on the nature of the query.

4.1.8. Checks must be done to ensure that patients have not opted out from the use of their data for research or planning purposes.

4.2. Disclosure of information

4.2.1. Disclosure of information is defined as:

> *Giving personal information in any way either to NCISH or University of Manchester employees, or to any other person or organisation except to the data subject. Disclosure to the subject is called subject access.*

4.2.2. In accordance with the advice from solicitors Beachcroft Wansbroughs (engaged by NCISH's previous Commissioners the National Patient Safety Agency in 2003), if NCISH is subpoenaed to disclose information on either living or deceased patients, this will be resisted. However, in those instances where disclosure of information is sought, despite resistance, information will be disclosed and used for no other purpose than the legal proceedings in respect to which that information is sought. In the case where a court deems it necessary:

- In the interests of litigation and the information could not be obtained elsewhere

- In relation to a police investigation

The response in full from Beachcroft Wansboroughs solicitors is filed with the Project Director (located in M:\Inquiry Management Information).

4.2.3. If a patient phones to request data about him/herself that might be held, the request will initially be directed to the Project Director who will inform the Senior Management Team and the advice of the University's Records Management, DP and FOI Office will be sought. The University's Information Governance Office will manage the response to the request. The outcome of the request and final decision taken should be clearly recorded.

4.2.4. If family members phone to request information on a deceased relative the request will initially be directed to the Project Director who will inform the Senior Management Team and the advice of the University's Information Governance Office will be sought. The University's Information Governance Office will manage the response to the request. The referral and outcome of the request will be recorded.

4.2.5. If an individual requests that information about themselves be withheld from someone, or some agency, which might otherwise have received it, the individual's wishes should be respected unless there are exceptional circumstances which include:

- When the information is required by statute or court order.
- Where there is a serious public health risk.
- Where there is a risk of serious harm to other individuals.

4.2.6. For the prevention, detection or prosecution of serious crime – disclosure of identifiable information may be justified e.g., in relation to the protection of children (under the Children's Act 1989 and in circumstances where there is knowledge or belief of neglect).

The decision to release information in these circumstances will be made following consultation, as appropriate, with the Senior Management Team and the University Information Governance Office. The advice of NCISH's lead mental health trust Caldicott Guardian (Greater Manchester Mental Health NHS Foundation Trust) may also be sought depending on the nature of the query.

4.3. Disclosure of information to the police

Police requests for disclosure of NCISH information should be referred to the Project Director who will inform the Senior Management Team and the advice of the University's Information Governance Office will be sought. The University's Information Governance, DP and FOI Office will manage the response to the request.

4.4. Disclosure of information to the media

All enquiries from the press or TV companies should be referred to the Project Director. Advice from the Senior Management Team will be sought as to the appropriate response.

5. General Data Protection Regulation (GDPR)

5.1. The General Data Protection Regulation

5.1.1. The GDPR was adopted on the 27th April 2016, and is enforceable from the 25th May 2018. The GDPR supersedes the Data Protection Act 1998.

5.1.2. The GDPR is focused on looking after the privacy and rights of the individual, based on the premise that individuals should have knowledge of what data is held about them, and how it is held.

5.1.3. Information on the GDPR and Data Protection is available from the Information Commissioners Office (ICO). Website address:

https://ico.org.uk

The ICO is responsible for the notification system.

5.1.4. As part of the University of Manchester, NCISH is obligated to operate according to the University's Data Protection policies and procedures.

5.2. Key elements

5.2.1. The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller. Notification is the process by which a data controller's details are added to the register. The ICO requires every data controller who is processing personal data to notify unless they are exempt. The website address as the public register for data controllers is as follows:

https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

5.2.2. Principles of the GDPR: Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate

5.2.3. The GDPR states that the controller shall be responsible for, and be able to demonstrate compliance with the principles. Control of NCISH data is shared between HQIP and the University of Manchester. HQIP review an NCISH Information Governance Checklist at every quarterly contract review meeting. This IG Checklist ensures that the GDPR principles are upheld. This continually evolving document, and supporting evidence, is located at G:\INQUIRY_info security\HQIP GDPR requirements.

5.2.4. The principles on which the GDPR is based, and with which University employees managing personal data must comply, are explained in full here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

6. Caldicott Guidelines

6.1. The Caldicott Guardian

6.1.1. In a report published by Dame Fiona Caldicott in (1997), standards for the management of confidential information and the **non-clinical** use of patient-identifiable information in the NHS were set down. While generally supporting the purposes for which patient information is used, the report called for improvements to be made in the way this information is handled and shared. A follow-up report on the Guidelines in 2013 further clarified when sharing information might be important for care; the most recent guidance is captured in 'A Manual for Caldicott Guardians' (2017).

6.1.2. Patient-identifiable information is personal information that can be traced back to a living individual. In some cases a post code or NHS number may be sufficient to trace an individual.

6.1.3. Two major concerns arising from a review between December 1996 and June 1997 were:

1. A variable awareness throughout the NHS of confidentiality requirements outside the clinical setting.
2. A need to ensure that information which can readily identify individual patients is kept to a minimum.

6.1.4. The Caldicott report mandated action to meet the following recommendations:

1. Every dataflow, current or proposed, should be tested against basic principles of good practice. Continuing flows should be re-tested at appropriate intervals.
2. A programme of work should be established to reinforce awareness of confidentiality and information security requirements amongst all staff within the NHS.
3. A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.
4. Clear guidance should be provided for those individuals/bodies responsible for approving uses of patient identifiable information.
5. Protocols should be developed to protect the exchange of patient identifiable information between NHS and non-NHS bodies.
6. The identity of those responsible for monitoring the sharing and transfer of information within agreed local protocols should be clearly communicated.
7. An accreditation system, which recognises those organisations following good practice with respect to confidentiality, should be considered.
8. The NHS number should replace other identifiers wherever practicable, taking account of the consequences of errors and particular requirements for other specific identifiers.
9. Strict protocols should define who is authorised to gain access to patient identity where the NHS number or other coded identifier is used.

10. Where particularly sensitive information is transferred, privacy enhancing technologies, i.e., encryption must be explored.

11. Those involved in developing health information systems should ensure that best principles are incorporated during the design stage.

12. Where practicable, the internal structure and administration of databases holding patient identifiable information should reflect the principles developed in the Caldicott report.

13. The NHS number should replace the patient's name on Items of Service claims made by General Practitioners as soon as practically possible.

14. The design of new systems for the transfer of prescription data should incorporate the principles developed in the Caldicott report.

15. Future negotiations on pay and conditions for General Practitioners should, where possible, avoid systems of payment, which require patient identifying details to be transmitted.

16. Consideration should be given to procedures for General Practice claims and payments, which do not require patient identifying information to be transferred, which can then be piloted.

6.1.5. From the recommendations came six good practice principles:

- **F**ormal justification of purpose.
- **I**nformation transferred only when absolutely necessary.
- **O**nly the minimum required.
- **N**eed to know access controls.
- **A**ll to understand their responsibilities.
- **C**omply with and understand the law.

6.1.6. In a follow-up report led by Dame Fiona Caldicott – 'Information: To Share or not to Share. The Information Governance Review' (2013), the challenge of protecting the patient or user's information, and when it might be appropriate to share information to improve care was examined. The review concluded that the original 6 principles were as relevant now to the NHS and social care system as when the first Caldicott report was published however an additional principle was included:

- The duty to share information can be as important as the duty to protect patient confidentiality. Explicitly – that health and social care professionals should have the confidence to share information in the best interest of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

6.2. Audit and research

6.2.1. In order to comply with the Caldicott guidelines all requests for patient-based information for research, audit, surveys, projects, questionnaires and work studies etc., must be referred in the first instance to the Project Director.

6.2.2. Patient-identifiable information should not be obtained directly from patients by those carrying out research/audit/survey/project etc., before Caldicott registration. NCISH has a formal agreement with the Caldicott Guardian of every mental health

trust from which it collects data. NCISH has local ethics agreements with trusts which should suffice.

6.2.3. When staff leave NCISH, all patient-identifiable information in their possession, including back-ups and copies, must be returned to NCISH, anonymised or deleted.

6.3. Case studies

6.3.1. Patient identifiers which feature in case studies must be effectively anonymised so that the patient is not identifiable from visual aids or case details.

6.3.2. If the patient's identity could be recognised or deduced, consent must be sought and documented in the case notes.

7. Legal Issues

7.1. Acts Having a Bearing on the work of NCISH

7.1.1. Many issues surrounding information systems security are governed by legislation. In 2003, the National Institute for Clinical Excellence (funders of NCISH at that time) engaged legal advisers Beachcroft Wansbroughs Solicitors to consider the confidential enquiries research in relation to a number of these Acts:

- The Data Protection Act 1998.
- Access to Health Records Act 1990.
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Police and Criminal Evidence Act.

NCISH legal advice from Beachcroft Wansboroughs solicitors is filed with the Project Director.

7.1.2. Other Acts include:

- Common Law Duty of Confidentiality.

  Common Law provides protection for information that has been provided confidentially. Information collected by health care organisations about present, past and future patients is confidential and has been made available for the purpose of providing health care. All staff are under an explicit obligation to preserve the confidentiality of this information.

- Copyright, Designs and Patents Act 1988.
- Computer Misuse Act 1990.
- Telecommunications Act 1984.
- The Crime and Disorder Act 1998.
- The Criminal Procedures and Investigations Act 1996.
- Electronic Communications Act 2000.
- Regulation of Investigatory Powers Act (2000).
- Health and Social care Act 2001 & revisions to Section 60 under the NHS Act 2006.
- Criminal Justice Act 1988.
- Contempt of Court Act 1981.
- Obscene Publications Act 1959.
- The Public Order Act 1986.

For further information, Appendix C, Legal Acts relevant to NCISH's research.

8. Risk Management

8.1. Objective

8.1.1. To identify, measure and counter possible threats to the security of information, communications and systems.

8.1.2. Provide a framework under which the assessment of risks is conducted.

8.2. Risk management rationale

8.2.1. The threats to which information and communication systems can be subjected continue to evolve, e.g. the introduction of new viruses; at the same time there are new technological developments that bring with them new security issues.

8.2.2. The information infrastructure is not static and it cannot be assumed that a past assessment will provide an accurate reflection of the current state. Each time a security risk assessment is conducted it should examine each information system used by the organisation.

8.2.3. For the Information Security and Management Policy to be effective it should keep in step with evolving threats and it is useful to periodically validate the applicability of security procedures through conducting a risk assessment.

8.3. Methodology

8.3.1. All systems will be subject to periodic security reviews by systems managers. The depth of a review will be determined by the importance and size of the particular system. The reviews would include but not be limited to:

- Checking that desktops/laptops have University approved and licensed software installed.
- Checking that desktops used by the CMHS that are connected to the CMHS's network do not have any confidential data stored locally on them. Laptops and any other such device that has internet access will not be connected to the CMHS network.
- Checking that desktops/laptops used by NCISH that are connected to the University network and the Internet do not have any confidential data stored locally on them.
- Checking office access security.

See Appendix D, Asset Audit Log.

8.3.2. The System Level Security Policy, Appendix I, will be reviewed on an annual basis to check that it is up to date and that system users are current.

8.3.3. The risk assessment should take a broad view, which includes the inter-relations between information systems. The starting point for the risk assessment is analysis of the information infrastructure to identify the systems, communications links and highlight the sensitivity of the data held. The information should be used to prioritise the order in which systems should be examined, according to a defined risk assessment schedule.

8.3.4. Any problems that are identified should be documented and incorporated into action plans for removing the weaknesses or introducing system or procedure change. This is documented in an NCISH Data Protection Impact Assessment (DPIA).

8.3.5. Reviews will include:

- Identification of assets of the system and their values.
- Evaluation of potential threats:
  - The sensitivity of the information being held on each information system.
  - The physical security of the accommodation within which information equipment is housed.
  - The physical hazards to which the system might be subjected (e.g., fire), including any additional hazards (proximity to danger areas, such as kitchens, rest rooms).
  - The ease with which non-authorised people could get access to information systems.
  - The potential for physical tampering (e.g., communication links).
  - The strength of access protection mechanisms (e.g., password protection) and whether users are following security procedures.
  - The security of all communication links to the system (e.g., use of encryption).
  - If the system audit trails (e.g., file usage logs) are being operated.
  - Whether users can electronically load data onto the system (e.g., copy files from floppy disk).
  - The reliability of data entry protection functions (e.g., data integrity checks).
  - The presence of unauthorised software (e.g., additional copies of a particular application).
  - The level of staff turnover and use of temporary staff.
- Assessment of likelihood of threats occurring, including the temptation towards fraud, which the particular system could offer and the extent to which professional hackers might wish to gain access.
- Assessment of the impact of an incident.
- Assessment of the security risks that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets.
- Identification of practical cost-effective counter measures/security requirements.

8.3.6. Systems are liable to independent reviews by internal and external auditors. The system was audited by the Health and Social Care Information Centre (HSCIC) in November 2015.

8.4. Reporting

Each system review will include a formal report to the Project Director containing findings and recommendations, who will then ensure that the necessary action is taken.

9. Asset Management

9.1. Objective

9.1.1. To protect University equipment and data against loss, misuse or damage and avoid interruption to business activity.

9.1.2. To ensure that each asset is managed and controlled appropriately.

9.2. Physical assets

9.2.1. An up-to-date register of all NCISH IT equipment and disposal of physical computer assets will be maintained by Research IT. This will include the approximate age, system details, location, and serial number. Research IT will be responsible for the maintenance of this part of the asset audit log. See Appendix D, Asset Audit Log.

9.3. Data Assets

9.3.1. An up-to-date register of all NCISH data assets will be maintained by the data asset owners. This will include the date of receipt of the data, the data asset owner, and the date of destruction of the asset. See Appendix D, Asset Audit Log.

9.4. Purchasing of IT equipment

9.4.1. All purchases must be made in consultation with Research IT and the Project Director.

9.5. System ownership

9.5.1. NCISH's information systems will be the responsibility of Research IT whose responsibilities will include ensuring compliance with the University's IT Security Policies, ensuring the appropriate use of the equipment, troubleshooting and maintenance. Research IT will identify all the assets within their area of responsibility and will determine:

- The use of the asset/equipment.
- What type of access each user is allowed.

9.6. Information ownership

9.6.1. The Project Director will assign responsibility of data assets to authorised NCISH staff. Authorised NCISH staff as the data owner, will be responsible for:

- Identifying all the data within his/her area of responsibility.
- Specifying how the data should be used.
- Agreeing who can access the data, and what types of access each user is allowed.
- Approving appropriate security controls.
- Ensuring compliance with the GDPR, and any other legislation covering personal or corporate data.

9.7. Equipment siting and protection

9.7.1. Equipment will always be installed and sited in accordance with the manufacturer's specification.

9.7.2. The primary server and a standby server are rack-mounted in a server infrastructure cabinet (locked at all times) in the main NCISH Office. The standby server is to provide business continuity in the case of any unforeseen event. Physical access to the server cabinet is strictly limited to the Research IT, authorised NCISH staff and authorised University of Manchester IT Services staff. The main NCISH office is locked out of hours and also when vacant. See Appendix I System Level Security Policy.

9.7.3. All PC monitors must be positioned so that any confidential information displayed will not be viewable by unauthorised personnel or the public.

9.8. Power supplies

9.8.1. An uninterruptible power supply (UPS) unit will be used to ensure that the CMHS primary server does not fail during a power cut. The CMHS servers will switch over to the UPS if there is a power cut. The UPS will allow the CMHS servers to shut down properly.

9.8.2. The UPS for the primary server will be configured to self-test every week. A log of the test can be viewed through the accompanying UPS software.

9.9. Equipment maintenance

9.9.1. The CMHS servers include maintenance on 5-year agreements depending on the Service requirements. Supplier engineers replace any defectives items and may request access to the primary/standby server. The Research IT and/or authorised University of Manchester IT Services staff will carry out component replacements on behalf of the suppliers where possible. See Appendix I System Level Security Policy.

If a situation arises whereby equipment needs to be sent off campus the IS&M Team will meet, and take advice where necessary, on the potential for any breach of security. NOTE: Confidential information is not held on portable PC equipment that might need to be sent away for repair.

9.9.2. The CMHS server hard drives will be covered by a “keep your hard drive option” in the warranties. This is so that if a hard drive fails, if it is replaced by the Supplier with a new one, the Supplier does not take the failed hard drive away with them but instead, it can be kept securely by Research IT until such a time that it can be securely destroyed in line with secure destruction of equipment procedures.

9.9.3. All computers and printers will be covered by maintenance agreements with third parties for repair of out of warranty equipment provided it is cost effective (each case will be judged on its merits). The IT Service desk will only make all such repairs on approval.

9.9.4. On-going maintenance arrangements (defining level of maintenance and minimum levels of performance) should be the subject of contractual agreement.

9.9.5. Equipment with accessible data on a hard disk should only be sent for off-site maintenance after all data have been transferred to another hard drive on the CMHS network, where possible. Hard disks should be electronically shredded where possible before being sent off–site for maintenance. Equipment or software should not be taken off-site without documented (signed) management authorisation.

9.9.6. Hardware repairs and upgrades to computers, printers and other IT equipment should only be undertaken by authorised staff. See 9.9.1 above and, Appendix I System Level Security Policy.

9.10. Prevention of theft and malicious damage

9.10.1. Wherever possible, IT equipment/assets should be out of the view of the general public. Where possible, the placement of equipment near large windows will be avoided and if this is not possible, equipment will be shielded with curtains, blinds etc.

9.10.2. Where necessary, security of IT equipment should be implemented with locks or security marked.

9.10.3. In vulnerable areas locks on windows should be fitted and used when the room is unoccupied.

9.10.4. Rooms containing computers that hold sensitive information must be locked when unoccupied. Smart card door security or combination locks are to be used whenever possible. Combination locks must have their codes changed regularly.

9.11. Prevention of misuse

9.11.1. All University IT equipment and information systems must be used for legitimate University business purposes only unless other purposes are approved by the Project Director.

9.12. Security of hard disks

9.12.1. Patient identifiable data should not be held on the hard drive of any laptop – see 9.12.3 below. Removal off site of such disks represents a potential threat to the University. Each case will be judged on its merits balancing the need versus the risk of breach of confidentiality and then only to approved repairers who have signed confidentiality agreements. Prior to moving off site, important data should be secured and temporarily backed up. Whenever possible the data should be overwritten using an approved, licensed security product.

9.12.2. All desktops on the CMHS network should be fully encrypted to AES-256 level which requires a minimum 10-character boot password before the operating system is loaded, to ensure that no data on the hard drive will be accessible when the desktops are disposed of or in the event that they are stolen. See Appendix I, System Level Security Policy.

9.12.3. Laptops should be encrypted in accordance with the University's guide on encryption – see https://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/laptop/

9.13. Security of equipment and data

9.13.1. Equipment and data will not be taken off site without formal approval by the Project Director or Administration Manager. No patient identifiable data is allowed off site. If there is a requirement to take data off-site, it must be anonymised and approved by the Project Director.

9.13.2. Staff borrowing equipment, are responsible for its safety and security.

9.13.3. Patient-identifiable, confidential or sensitive information should not be placed on privately owned computers, laptops, portable hard drives, USB pens/sticks, mobile phones, tablets or any other form of personal portable media.

9.13.4. Portable PCs are very vulnerable to theft, loss or unauthorised access. Security measures must have been implemented - see Section 9.12.3.

9.13.5. To preserve the integrity of data, no patient identifiable data may be stored on portable PCs/laptops. They should be maintained and backed-up regularly and batteries kept charged to preserve their availability.

9.14. Disposal of equipment

9.14.1. Computer and printer hardware disposal can only be authorised by the Project Director, Information Governance Officer or Research IT. Disposal will be undertaken by Research IT or authorised IT Services staff. Prior to disposal, the hard drives of both desktops and laptops will be securely erased using University approved software.

9.14.2. See Appendix I System Level Security Policy for details on the process for decommissioning IT hardware and backup tapes.

9.14.3. IT equipment will be replaced by new equipment approximately every five years in order to keep NCISH's systems and software up to date.

9.15. Asset loss and data loss

9.15.1. In the event that equipment or data assets are destroyed, e.g. fire, or loss due to theft, the Project Director will lead the investigation / notification process supported as appropriate by the Information Governance Officer, Research IT and Senior Management Team depending on expertise / authority required. See Appendix E Asset Information Loss. See also Section 20, Security Incident Management.

10. Software Management

10.1. Objective

10.1.1. To comply with the law on licensed products.

10.1.2. To maintain version control.

10.1.3. To minimise the risk of computer viruses.

10.1.4. To reduce the risk of misuse of University equipment.

10.1.5. To minimise system malfunction, maintain integrity and avoid disruption or service.

10.2. Software

10.2.1. An up-to-date register of all software will be maintained for NCISH to ensure that NCISH is aware of its assets and that licence conditions are followed. See Appendix D Asset Audit Log.

10.3. Licensed software

10.3.1. All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action. Licenses for any software that is not covered by a University Campus Agreement will be held by Research IT.

10.3.2. Only software that has been obtained from authorised suppliers is to be loaded onto the University network or computers.

10.3.3. All software must be installed by Research IT or other approved IT Services staff.

10.3.4. It is Research IT 's responsibility to ensure that the software pertaining to their system is being used within the terms and conditions of the software licence.

10.3.5. Software will not be placed on network servers or on multiple machines unless this is in accordance with the licensing agreement.

10.3.6. Any NCISH staff learning of any misuse of software or related documentation within NCISH shall notify their line manager.

10.4. University software standards

10.4.1. Where the University has an approved software solution, (a campus wide license agreement), for a particular requirement, this will be used. See the Applications section on the University IT services website, https://www.itservices.manchester.ac.uk/software/.

10.4.2. The University will require the use of specific general-purpose packages (e.g., Microsoft Office) to facilitate support and staff mobility. Non-approved packages should be phased out as soon as practicable.

10.5. Software updates to site systems

10.5.1. Inadequately controlled changes to application software are a common cause of system or security failures. Formal management responsibilities and procedures are therefore necessary to ensure satisfactory control of all software or procedures.

10.5.2. Proposed changes should only be approved by Research IT, when:

- Funding for the change and any additional maintenance costs has been agreed and authorised.

- The changes requested do not alter, degrade or compromise, system controls, security, access rights or data integrity.
- The changes requested do no alter or compromise the integrity of other system(s).

10.5.3. Appropriate full back-ups will be required prior to any upgrade.

10.5.4. Backups of the original version should be retained until the new version has been tested, installed and operationally live for a minimum of 1 month.

10.5.5. All new versions should be implemented in a test environment and detailed testing should be completed prior to upgrading the live system.

10.5.6. Users must be given adequate warning of any interruption to the service that may result from the update install.

10.6. Quality assurance

10.6.1. Research IT should ensure sufficient user acceptance testing to identify any operational and security issues arising from the upgrade.

10.6.2. Research IT will be responsible for acceptance testing the software change to ensure that current requirements continue to be met, and that any new features are tested to ensure functionality. Research IT will 'sign off' the upgrade when they are satisfied that the upgrade is complete and successful.

10.7. Virus control

10.7.1. The University seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software.

10.7.2. Anti-virus software will be installed on all CMHS networked PCs and NCISH (University networked) laptops.

PCs and laptops that are not connected to the CMHS network will be connected to the University network and will be in the University active directory. This will ensure that anti-virus updates are automatically downloaded as well as any operating system updates.

Research IT will be responsible for downloading the latest anti-virus definition files from a University network connected PC/laptop onto a USB stick and then transferring those files to the appropriate location on the CMHS network. PCs connected to the CMHS network will be configured to automatically download any new anti-virus definition files when users' logon to the network.

In the absence of Research IT, the same NCISH staff who have been authorised to check the overnight backup will be responsible for downloading the latest anti-virus definition files and placing them into the appropriate location on the CMHS network. See Appendix G, Backup Procedure for who these staff are.

10.7.3. E-mails from an unknown source should be carefully examined. Suspect attachments should not be opened.

10.7.4. Users should report any viruses detected/suspected on their machines immediately to Research IT or the IT Service desk.

10.7.5. No newly acquired media from whatever source are to be loaded unless they have previously been virus checked by a locally installed and approved virus-checking package. This is particularly important with shareware or public domain disks.

10.7.6. Programmes and files that have been downloaded from the Internet should be virus checked prior to installation or use.

10.7.7. Microsoft ended the Extended Security Update (ESU) Program on 10th January 2023 so no further security updates will be provided for Windows 7.
Therefore, Research IT can no longer be responsible for keeping Windows on the CMHS PCs up to date.

11. User Access Control

11.1. Objective

11.1.1. To control an individual's access to systems in accordance with their job function.

11.1.2. To modify access levels when staff changes jobs, functions or leave NCISH. The University procedures on this issue will be followed.

11.2. Registering users

11.2.1. Formal procedures will be used to control access to University systems. Access to NCISH's systems will be approved by the Project Director and implemented by Research IT.

11.2.2. Research IT will continually modify or remove access privileges to the CMHS's network as appropriate in consultation with an appropriate line manager, when an individual's responsibilities change or they leave the employment of the CMHS.

11.2.3. Active Directory User groups have been set up on the CMHS network that restricts user access to shared folders/and or NCISH SQL Server databases on the network. Shared folders on the CMHS network will contain information relating to certain areas of NCISH. Not all users will be required to have access to all shared folders or NCISH SQL Server databases. The Project Director will approve users' memberships of Active Directory User groups that are relevant to a user's job requirements.

11.2.4. Visitor access will be approved by the Project Director and implemented by Research IT. The Project Director will approve visitors' memberships of Active Directory groups that are relevant for their visit.

Staff who have been authorised to access NCISH's systems will not logon to the CMHS network using their own username and password in order to grant a visitor access to the CMHS network. Visitors will use their own username and password to access the CMHS network.

11.3. User password management

11.3.1. Only authorised CMHS staff will have active directory user accounts and login permissions to the CMHS network. Different projects are allocated shared folders on the CMHS network – each project may have more than one shared folder. Permissions to access shared folders on the CMHS network or any SQL Server databases are controlled by Active Directory User groups. Users will have access to projects and SQL Server databases depending on which Active Directory User group they are members of. The Project Director will approve users' memberships of Active Directory User groups that are relevant to a user's job requirements – see Section 11.2.3 above.

11.3.2. All passwords will be specific to individuals and must not be disclosed to others.

11.3.3. No individual will be given access to a live system unless properly trained and made aware of their responsibilities for security and data accuracy.

11.3.4. No user should be allocated a password until they have signed NCISH's confidentiality agreement.

11.3.5. Passwords must be changed regularly – all new systems must include password ageing to force users to change their password periodically. This should never exceed six months and the recommended period is 90 days or less.

11.3.6. Passwords must be changed whenever there is any indication of possible system or password compromise.

11.3.7. In certain circumstances, e.g., when a member of the Research IT team or member of the IS&M Team staff is suspended or dismissed, all access codes and administrator passwords must be changed immediately. Access to the corridor at the Centre for Mental Health and Safety should be removed.

11.3.8. No access should be automated.

11.3.9. A password protected screen saver will be activated on all CMHS networked PCs after a period of inactivity of 10 minutes.

11.3.10. Users should be required to enter a password when a University networked PC/laptop wakes from sleep.

11.3.11. Users should lock their University networked PC/laptop when it is unattended i.e. using CTRL + ALT + DEL so that a password must be entered to unlock it.

11.3.12. In the event of "forgotten" passwords, Research IT should provide a fast and secure method of reallocating access.

11.3.13. All key user accounts and passwords must be sealed and kept in a fireproof safe. Access to these user accounts and password should be restricted to authorised NCISH staff only.

11.4. Special privilege management

11.4.1. 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.

However, additional privileges may be granted to a member of staff for a specific time period to undertake a particular function. This should be requested by the user's line manager and implemented only after approval by the Project Director or Information Governance Officer and Research IT. Privileges will not be granted until the authorisation procedure is complete. The IG Officer will keep a record of all special privileges granted and ensure access is terminated by Research IT at the appropriate time.

11.5. User passwords

11.5.1. Staff should ensure that:

- Previously used passwords must not be used. Passwords should not be easily guessable (e.g., "password") or one associated with the user (e.g., spouse's name) – nor one so complicated that it cannot be remembered.
- Passwords must meet complexity requirements i.e.

  Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

  Contain characters from three of the following four categories:

  English uppercase characters (A through Z

  English lowercase characters (a through z)

  Base 10 digits (0 through 9

  Non-alphabetic characters (for example, !, $, #, %)

- Passwords are never written down, unless this can be stored securely.

- Passwords are at least ten characters in length and include a mix of alphanumeric characters as they are more secure.
- Change temporary passwords at the first log-on.

11.6. Logging procedures

11.6.1. A log of all successful and failed login attempts will be kept.

11.6.2. Users must log off and shutdown the PC when leaving a PC at the end of a working day.

11.7. Transaction log

11.7.1. Internal audit arrangements will include:

- A log of all successful and failed logon attempts onto the primary server
- A log of corridor access – see Appendix I, System Level Security Policy

11.8. Encryption

11.8.1. Data transported to remote sites by computer media, should be encrypted where possible and/or password protected.

11.8.2. Encryption keys should be subject to password constraints. This restricts the chance of data being readable in the event of it being accidentally or intentionally intercepted.

11.9. Network

11.9.1. No unauthorised equipment should be connected to either the University network or the CMHS network. See https://www.itservices.manchester.ac.uk/wireless/ for more information on the University's Wireless (Wi-Fi) Service and access restrictions for connecting to the University network.

11.9.2. No privately owned computers should be connected to the CMHS network. Visiting clinicians will use any available PC on the CMHS network when there is a requirement for them to use the network.

Wireless access is available on campus which will allow privately owned computers to connect to the university network. See https://www.itservices.manchester.ac.uk/wireless/ for more information on the University's Wireless (Wi-Fi___33) Service and access restrictions for connecting to the University network.

11.9.3. Laptops and any other wireless enabled portable devices, such as, but not limited to smart phones, should not be connected to the CMHS network.

11.10. Facsimiles

11.10.1. Patient's names and/or addresses must not be faxed with clinical details.

11.10.2. Pre-programmable fax dialling codes must be used where available to guard against incorrect dialling. Pre-programmed numbers should be tested before use is authorised.

11.10.3. Any party who is not an intended recipient should make no use or reliance on the contents of a fax.

11.10.4. Only the minimum amount of information for the purpose required should be sent.

11.10.5. Fax machines must not be positioned in “public areas”.

11.10.6. A fax header sheet must be used to identify the intended receiver and declare the confidential nature of the information; furthermore, a contact number must be included for anybody who thinks they are the wrong recipient of said data. The NCISH standard fax header sheet must be used wherever possible.

11.10.7. All faxes must display a valid disclaimer. A disclaimer should be added to each fax to ensure that any recipient is aware of its confidential nature and that it should be deleted if received in error. An example:

> IMPORTANT:
>
> This transmission is intended for the above addressee only. It may contain legally privileged and confidential information. If you are not the intended recipient you are hereby notified that if you receive this transmission, any distribution or copying is strictly prohibited. If you have received this facsimile in error, please notify us immediately by telephone on the above number and return the original by post to the sender at the above address.
>
> Thank You.

11.11. Contractors/temporary personnel

11.11.1. All contractors, agency and temporary staff are subject to the same security standards as permanent staff.

11.11.2. Such personnel, given access to sensitive information held on computers, must sign a confidentiality agreement.

11.11.3. Adequate training, in keeping with the designated responsibilities and risks must be given prior to authorising access.

12. Network Security

12.1. Objective

12.1.1. To ensure that appropriate controls are established to ensure the security of the data held within the CMHS network.

12.1.2. To protect the CMHS network from unauthorised access.

12.1.3. To ensure the continuity of CMHS network services including servers.

12.2. Network security controls

12.2.1. Research IT should ensure that appropriate controls are established to ensure the security of the data held within the CMHS network, and the protection of connected services from unauthorised access.

12.2.2. Operational responsibility for the CMHS network should be separated from computer operations, where appropriate.

12.2.3. All authorised PCs that are connected to the isolated network will have their hard drives fully encrypted to AES-256 level encryption.

Where TrueCrypt is used to encrypt a PC, the full system encryption requires that a 20+ character passphrase is entered before the PC loads the operating system.

As CMHS PCs are replaced or any new PCs added to the CMHS network, these will be fully encrypted to AES-256 level encryption using Bitlocker.

Where Bitlocker is used to encrypt a PC, the full system encryption requires that a 10+ character boot password is entered before the operating system is loaded.

This passphrase/password is known only to authorised users of the PC.

Once the PC has loaded the operating system an active directory username and password account is required to login to the PC. This account is unique to each authorised member of staff and only the account owner knows the password.

All PCs have the Window firewall enabled and configured to prevent remote access.

The PCs have been configured to automatically update their antivirus signatures daily via an update repository hosted on the isolated server.

13. Intranet/Internet Access

13.1. Objective

13.1.1. To ensure that Intranet/Internet access is used appropriately and there is no compromise to the security of University systems and the confidentiality of information. See the University's acceptable use policy for the use of IT facilities and services for staff, https://www.itservices.manchester.ac.uk/aboutus/policy/.

13.2. Central control of Internet sites

13.2.1. General computer and network usage of the University network may be monitored in accordance with University guidelines and policies. See the University's standard operating procedure for the authority to access and monitor University Account holder communications and data, https://documents.manchester.ac.uk/DocuInfo.aspx?DocId=16278.

13.3. Unintentional breaches of security

13.3.1. If Internet users unintentionally find themselves connected to a site which contains sexually explicit or otherwise offensive material, they must disconnect from the site immediately and inform the IT Service desk.

13.4. Issue of Internet access

13.4.1. Before use may be made of computing or networking facilities in the University, students and staff of the University must register as a user – the University's procedures for registering users will be followed.

13.5. Non-permissible Internet access

13.5.1. **Users must obey University policy on internet access.** See the University's Acceptable Use of IT Facilities and Services policy for Staff, https://www.itservices.manchester.ac.uk/aboutus/policy/.

- The Internet or university e-mail **MUST NOT** be used to transmit patient identifiable personal data.

13.6. Quality of information

13.6.1. Users should be aware that information on the Internet may not be reliable or up to date and should be treated with caution. Staff should ensure that, prior to use, information from the Internet should be credible, in date and authentic.

14. Web Publishing

14.1. Objectives

14.1.1. To ensure that information published on the Internet and Intranet meets all security and confidentiality standards.

14.1.2. To ensure that information published on the Internet and Intranet meets University branding and layout standards. This will be done using the University's content management system.

14.2. Web publishing

14.2.1. All material published to the World Wide Web or the University Intranet, must be approved by the Project Director.

14.2.2. Person-identifiable confidential information must not be published on a web site.

14.2.3. Staff are not permitted to create their own web site in the name of the University or NCISH.

14.2.4. The website must not contain any information that is not directly related to the Centre's research programmes and must not contain material linked with any improper or unlawful activities, including:

- Libellous or defamatory statements.
- The display of pornographic material.
- Racist comments or the incitement of racism.

14.2.5. Information held on websites or the Intranet must not be used to promote personal business or to provide personal or financial gain, except as may be permitted by University policy and procedures.

14.3. Copyright

14.3.1. Contents of all electronic publications must follow University and the Healthcare Quality Improvement Partnership's standards regarding copyright legislation. Publishers must secure permission when including copyright or trademark material, such as, text, photographic images, and video or graphic illustrations.

14.3.2. Publishers should be aware that publishing material on the web page would put that material into the international domain. It would be prudent to include an assertion of any relevant intellectual property rights, such as a claim to copyright.

14.4. Intranet

14.4.1. Staff who create and publish pages of information for the University Intranet are responsible for its content and ensuring that their pages are kept up to date.

14.4.2. Staff who create and publish Intranet pages must comply with security and confidentiality standards and University policies and procedures.

15. E-mail

15.1. Objective

15.1.1. To ensure that e-mail services are used appropriately and there is no compromise to the security of University systems and the confidentiality of information. See the University Guide to email and sensitive data, https://www.itservices.manchester.ac.uk/email/staffemail/safe/confidential/ and https://www.itservices.manchester.ac.uk/cybersecurity/data-handling/

15.2. Security and confidentiality

See the University Guide to email and sensitive data, https://www.itservices.manchester.ac.uk/email/staffemail/safe/confidential/ and https://www.itservices.manchester.ac.uk/cybersecurity/data-handling/

See the University's advice on encryption software, https://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/

See also the University guides:
to data handling
to email and sensitive data
to protecting data using encryption
https://www.itservices.manchester.ac.uk/cybersecurity/data-handling/

15.3. Legal issues

15.3.1. E-mails are considered legal documents. Misuse may contravene one or more of the following:

- General Data Protection Regulation.
- Computer Misuse Act 1990.
- Law of Copyright.
- The Electronic Communications Act 2000.

15.4. Authorised e-mail

15.4.1. E-mail sent externally will carry the authority of the University. Users are required to maintain the same literary standards as those used on letter headed paper and the same degree of politeness.

15.5. Disclaimer

15.5.1. A disclaimer should be added to each e-mail centrally to ensure that any recipient is aware of its confidential nature and that it should be deleted if received in error. Any party who is not an intended recipient should make no use or reliance on the contents of the e-mail. An example:

15.6. Users responsibilities

15.6.1. E-mail users must NOT:

- Send patient identifiable information into or over the Internet. Where there is a need to exchange data with Trust contacts, the procedure to be followed is detailed in Appendix I, System Level Security Policy.
- Create, access or send any offensive, obscene or indecent images, data or other material, or any data capable of being converted into obscene or indecent images or material.
- Use the e-mail systems for any use other than University business unless authorized.
- Create or send any messages that may constitute any form of harassment including racial or sexual harassment.
- Create or send any material that is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Create or send any defamatory or libellous material.
- Send any material that may infringe on the copyright of another person or company.
- Send any unsolicited commercial or advertising material either to other users or organisations connected to other networks.
- Initiate or propagate electronic chain letters.
- Send mail to randomly selected recipients.
- Send multiple messages unnecessarily i.e., spamming.
- Forge or anonymously send mail.
- Undertake any actions that are intended to use unreasonable system resources or otherwise interfere with other users' ability to utilise the local network.
- Make any attempt to infect other systems with computer virus.
- Use e-mail to promote personal business or to provide personal or financial gain, except as may be permitted by University policy and procedures.

See the University Guide to email and sensitive data, https://www.itservices.manchester.ac.uk/email/staffemail/safe/confidential/

15.7. Use of e-mail addresses

15.7.1. Only University or NHS e-mail addresses may be placed on University documentation and letterheads.

16. Portable Electronic Devices

16.1. Objective

16.1.1. To ensure that the additional risks associated with portable electronic devices, are addressed and minimised.

16.1.2. To ensure that no staff hold ANY person and patient-identifiable information on portable equipment.

See Appendix A; Glossary of Terms for a definition of a portable electronic device. Although patient identifiable data will not be held on portable equipment, where other types of sensitive data is held on portable devices, see the University's guide to encryption and data handling on https://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/.

16.2. Portable devices

16.2.1. Portable electronic devices represent a heightened risk regarding their physical security because:

- They are relatively more valuable than desktop personal computers and therefore are more attractive to thieves.
- Due to their portability they are more likely to be left in less secure locations.

Therefore, the following measures should be taken:

- No holding of ANY patient or person-identifiable information on a portable device.
- The operating system on laptops should be the University recommended operating system (currently Windows 10 or Windows 11) due to its superior security.
- The device must be encrypted to the minimum standards required by the University and there should also be passwords on screensavers.
- Data should normally be backed up to a separate device (such as encrypted magnetic tape data storage compatible with the CMHS servers and backup software), so that in the event of computer loss, the data is safe. Backup tapes must be stored in a safe in an NCISH office or in an off-site safe. If there is a requirement to backup data to other portable media (such as an encrypted USB stick/disks/DVDs/CDs/portable hard drive in the event that the backup software fails), the media/data must be encrypted/password protected and must also be stored in the safe in an NCISH office. When the backup on the media is no longer required i.e. normal backup procedures have been restored, the backup on the media must be securely erased and the media securely destroyed.
- The high incidence of car theft makes it inadvisable to leave portable equipment in a car, even when locked away in the boot.
- Any laptop provided by the University will only be used by authorised staff and used for University business.
- Any portable device that is stolen or mislaid must be reported immediately to the IS&M Team with a list of data stored on it.

16.3. Privately owned portable devices

16.3.1. It is not allowed for any staff to process patient-identifiable information on their personally owned equipment.

16.4. Storage media

16.4.1. In general, it is not allowed for any member of staff to have any patient-identifiable data taken off-site using unencrypted storage media, e.g., floppy disks, CD's, USB sticks, portable hard drives etc. However, backup tapes must be taken off site to be securely stored in a safe. The backup tapes should be encrypted. If a portable hard drive is used to backup data for reasons such as tape drive failure on the CMHS primary server, the backup on the portable hard drive must also be encrypted.

16.4.2. Additionally where there is a requirement to transfer patient identifiable information between the NCISH secure server and NHS Trusts via NHSmail an encrypted USB stick must be used. The encryption level of the USB stick must conform to NHS Information Governance data encryption standards –see https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance. See also Appendix I, Security Level Policy for details on the procedure of sending and receiving sensitive data via secure email.

17. Access Control to Secure Areas

17.1. Objective

17.1.1. To minimise the threat to the University's computer systems through damage or interference.

17.1.2. To prevent unauthorised access to the CMHS's network and information systems.

17.2. Physical security

17.2.1. In restricted areas, unrecognised or unaccompanied visitors should be challenged and escorted back to their host or a security representative.

Restricted areas include

- The 2nd floor of the Jean McFarlane Building. The corridor where the CMHS staff offices are located is swipe card access controlled. Clearance is required to have a University staff card enabled for access to the CMHS corridor. (This is overseen by the IG Officer. In the absence of the IG Officer, corridor access can be requested from the University Access Control Manager – see Appendix A, Glossary of Terms.) Only CMHS, Forensic Psychiatry and other University staff with a legitimate requirement to access the corridor have their swipe cards authorised to allow entry. Swipe card access to the corridor is audited annually by the IG Officer – see Appendix D, Asset Audit Log. CMHS offices are locked out of hours and also when vacant.

- The server cabinet in the main NCISH Office. This room is locked outside normal office hours and also when vacant.

Access to the cabinet is restricted to Research IT. In the absence of Research IT, certain members of NCISH staff will be authorised to access the server cabinet in order to check the daily backup – see Appendix G Backup Procedure for details of these authorised staff. In the absence of Research IT, as well as authorised NCISH staff members, IT Services staff will also be authorised to access the server cabinet in the event that Business Continuity has to be carried out – see Appendix H Business Continuity Guide, Terminology section on who these authorised staff are.

17.2.2. Authenticated representatives of third-party support agencies will only be given access through specific authorisation from the Project Director.

18. Security of Third-Party Access

18.1. Objective

18.1.1. To enable the University to control external access to its systems. See also the University's guide to protecting PCs and general advice, https://www.itservices.manchester.ac.uk/cybersecurity/advice/.

18.1.2. To minimise any risks to University assets or compromise of University services.

18.1.3. To enable the CMHS to control external access to its network.

18.2. Access control

18.2.1. No external agency will be given access to the CMHS's network unless that body has been formally authorised to have access.

18.2.2. External agencies will only be allowed access to the hardware/systems for which they are responsible.

18.2.3. NCISH will not allow unauthorised access to its systems.

18.3. Remote access

18.3.1. Remote access to the CMHS's network will not be allowed.

19. Audio Recordings

19.1. Objective

19.1.1. To safeguard the confidentiality of multimedia information such as photographs, slides, videos, audio tape, digital audio recordings.

19.1.2. To ensure appropriate storage and security of such records.

19.1.3. To ensure that the University can fully comply with subject access requests.

19.2. Introduction

19.2.1. Multimedia recordings made for research purposes are subject to confidentiality and security safeguards.

19.2.2. Specific written consent must be obtained prior to any multimedia recording that may identify individuals participating in a study. Participants must be informed of their right to withdraw consent at any time.

19.3. Multimedia recordings

19.3.1. Multimedia recordings may be used for research purposes, in adherence to the following guidelines:

In advance of the event:

- The subject must be informed and understand the reason, specified purpose and storage arrangements for the photograph or recording.
- Prior to the recording taking place, the subject must sign the appropriate consent form.
- Explicit consent must be given in advance of the recording being used within a public setting, e.g., conference presentation.

After the event

- The photograph/recording must be stored securely as a confidential record.
- In emergency situations, subjects unable to give consent in advance must be informed after the event and made aware of their right to object.

19.4. Storage and labelling

19.4.1. The recording must be stored securely in a reliable and traceable system. This will facilitate retrieval in the event of a subject access request.

19.4.2. When labelling patient multimedia recordings, the Data Protection and Caldicott implications must be considered and only the **minimum** identifiers necessary should be used. These may include one or more of the following, as appropriate:

NHS number; hospital number (or other unique identifying number); date; male/female; clinical details; name; initials; date of birth.

19.5. Recordings from which the patient cannot be identified

19.5.1. When the patient will not be identifiable from the recording, and it is to be used only within a research setting, only an oral explanation of the purpose of the recording is required. It should be recorded that the subject has given consent. The recording must not be used for any additional purpose without seeking specific consent from the subject.

20. Security Incident Management

20.1. Objective

20.1.1. To detect, investigate and resolve any suspected/actual security or confidentiality breach.

20.1.2. To manage security incidents to their logical conclusion.

20.1.3. To improve the development of the CMHS security procedures.

20.2. Security incidents

20.2.1. A security incident is an event that may result in:

- Degraded system integrity, i.e. data inaccuracy.
- Loss of system availability or degradation/disruption to University services.
- Unauthorised access to information or systems, e.g., patient records or pornographic/inappropriate websites.
- Unauthorised disclosure of confidential information.
- Unauthorised installations of hardware or software and breaches of licensing regulations.
- Financial loss or fraud.
- Embarrassment/ loss of reputation to NCISH or the University.
- Legal action.

Examples include:

- Any breach or attempted breach of the 'Information Security and Management Policy'.
- Virus discovery.
- Unauthorised access to systems – including failed log-in attempts.
- Theft of hardware or software.
- Theft of data/information.
- Unauthorised manipulation of data.
- Selling of data/information.
- Unauthorised installation of hardware or software.
- Access to or processing of pornography – or other inappropriate sites.
- Sabotage.
- Fraud.
- Denials of service.
- Use of hacking tools.
- Breach of copyright.

20.3. Responsibilities

20.3.1. Any member of staff on discovering a security incident must report it immediately to Research IT and the Project Director.

20.3.2. The Project Director will notify the Senior Management Team. If required by the incident, the University's Standard Operating Procedure on Information Security and data Protection Incident Reporting at https://documents.manchester.ac.uk/display.aspx?DocID=15678 will be followed. See Appendix E Asset/Information Loss and Appendix I System Level Security Policy. See also https://www.staffnet.manchester.ac.uk/igo/data-protection/report-data-protection-incident/.

20.3.3. Research IT and the Senior Management Team will initiate an investigation in conjunction with University colleagues.

21. Information Sharing Protocols

21.1. Objective

21.1.1. To ensure that information is disclosed in accordance with the Caldicott recommendations, GDPR legislation and other legal or local requirements.

21.1.2. Medical information is classified as 'sensitive' information. Therefore extra precautions must be taken before this information is disclosed to third parties, particularly non-NHS organisations who may not be obliged to comply with the Common Law 'Duty of Confidence'.

21.2. Information Sharing Agreements

21.2.1. Prior to disclosing person or patient-identifiable information to any **external** organisation to the University a signed protocol should be in place. This will ensure that external organisations pledge that the information obtained will be protected in accordance with statutory requirements.

21.2.2. Before information is disclosed, the information flow should be identified and any boundaries or conditions for processing should be identified. Consideration must be given to any possible future disclosures that may take place by the recipient of the information.

21.2.3. For an example of the Information Sharing Protocol with Trusts see Appendix F, Information Sharing Protocols (example of generic document).

22. Housekeeping

22.1. Objective

22.1.1. To maintain the integrity and availability of information/computer assets.

22.2. Record retention

22.2.1 All documentation related to NCISH data processes, minutes of meetings and details of formal decision making will be retained for not less than 6 years from the end of NCISH (minimum requirements set out in the Agreement for provision of the Clinical Outcome Review Programme (CORP) Mental Health signed with the National Patient Safety Agency, 2011 (subsequently transferred by the NPSA to HQIP, 2011)). NOTE: the document Records Management: NHS Code of practice (2009) states that data collected in the course of research should be retained – 'for an appropriate period to allow further analysis by the original or other teams subject to consent, and to support monitoring by regulatory and other authorities'. The Scottish Government Records Management: NHS Code of Practice (Scotland), version 2.1, January 2012 states that 'research records other than those of clinical trials that are the source data for the research' must be retained for 30 years.

22.2.2 Some NCISH data providers have specified data retention periods and data destruction schedules as a condition of receipt of data. Greater Manchester Police Force, providers of Police National Computer data, have specified that in the event NCISH ceases operation, all identifiable case information provided by the PNC will be destroyed immediately and all non-identifiable information will be destroyed after 1 year.

22.2.3 In the event NCISH ceases operation NCISH will consult with funders and data providers on the retention of identifiable and non-identifiable data and act accordingly.

22.2.4 Electronic and physical records reaching their destruction date will be documented and authorization for their secure destruction will be signed off by the Director for the Centre for Mental Health and Safety.

22.3. Data back-up

22.3.1. The backup procedure that has been adopted for the CMHS network infrastructure follows the grandfather, father, son model – see Appendix G, Backup Procedure.

Each week, every Monday, Tuesday, Wednesday and Friday, the system is backed up to separate tapes (magnetic tape data tapes i.e. LTO data cartridges) and these tapes are rotated the following week. The tapes are stored in the large datasafe in the main NCISH office in the Jean McFarlane building. Only authorised NCISH staff has access to the safe.

For the first 3 Thursdays in a month, the system is backed up to 3 different tapes each labelled Thursday 1, Thursday 2 and Thursday 3. These tapes are rotated on a monthly basis and are taken off-site to the Alan Turing Building to be stored in a safe within the IT Area Support office. Only authorised NCISH and Research IT staff have access to this safe.

Each fourth Thursday in a month, the system is backed up to tapes labelled Monthly 1, Monthly 2 and Monthly 3. Each of these tapes is rotated every 3 months and kept off-site in a safe in the IT Area Support office within the Alan Turing Building.

Each fourth month, the system is backed up to tapes labelled Quarterly 1, Quarterly 2, Quarterly 3 and Quarterly 4. Each of these tapes is rotated every 64 weeks and kept off-site in a safe within the IT Area Support office within the Alan Turing Building. Only authorised NCISH staff have access to this safe.

The CMHS storage infrastructure is hosted on an isolated primary with a (second) standby server in place. The standby server is a domain controller within the active directory and will be used for business continuity in any unforeseen events where the primary server becomes unavailable.

22.3.2. An electronic record of backups will be maintained that specifies which member of staff has checked the backup. See Appendix G, Backup Procedure for the records of backups.

22.3.3. All back-up media such as data tapes/data cartridges must be used within the manufacturer's specification. A record will be kept of the use of the media. See Appendix J, Backup Tapes Log.

22.3.4. All laptop users are advised to back-up their data regularly to the University network/DVDs/CDs/external hard drive (confidential data will not be stored on laptops) with a minimum 3-day cycle (preferably 5) before backups are overwritten.

22.3.5. Regular back-up copies of data should be undertaken, at the frequencies required by the particular system. Where feasible, automatic timed back-ups should be used. See Appendix G, the Backup Procedure.

22.3.6. All systems should have a member of staff clearly identified as responsible for the systems back up of data. Research IT will be responsible for the backup of data on the CMHS network and in his/her absence, authorised members of NCISH team will be responsible for the backup of data.

22.3.7. A regular check should be made to ensure the back-up and restore process is fully functional and data are backed-up as required. A record of such checks and of the back-ups must be maintained.

22.3.8. All backup tapes/disks will be held in secure locations. All on-site backup tapes will be stored in a datasafe i.e. a fireproof safe that is designed to store magnetic media (as magnetic media can become corrupt at 52°C).

Daily backup tapes will be stored in the large datasafe in the main NCISH office. Depending on which of the Weekly/Monthly/Quarterly backup jobs is due to run next, the appropriate tape (for that Weekly/Monthly/Quarterly backup) will also be stored in the large datasafe in the main NCISH office.

All other Weekly/Monthly/Quarterly backup tapes will be stored in a safe held in a secure off-site location which is currently the IT Area Support Office within the Alan Turing Building.

Passwords/encryption keys for the backup tapes will be stored separately to the backup tapes in sealed envelopes in a fireproof safe. See Appendix G, Backup Procedure.

22.3.9. Back-up and maintenance procedures must be adequately documented to enable other technical staff to understand and comply with the requirements.

22.4. Media disposal

22.4.1. All data storage media (floppy or hard disks, CDs, tapes, USB sticks, portable hard drives, backup tapes or other storage device) must be destroyed before disposal. See Appendix I, System Level Security Policy which details how this should be done.

22.5. Disposal of confidential waste

22.5.1. Paper waste of patient-identifiable information must be disposed of by crosscut shredding or pulping.

22.5.2. Electronic waste should be shredded using appropriate software.

23. Business Continuity Planning

23.1. Objective

23.1.1. To be able to restore the CMHS's network facilities to maintain essential business activities following a major failure of the primary server.

23.2. Need for effective plans

23.2.1. NCISH recognises that some form of server failure may occur, despite precautions and therefore seeks to contain the impact of such an event on its core business through a tested business continuity guide. See Appendix H Business Continuity Guide. The objective of the business continuity guide is to get users of the CMHS network up and running again as soon as possible in the event of the CMHS primary server failing.

23.2.2. NCISH requires tried and tested business continuity guides for its network facilities to be maintained.

23.3. Planning process

23.3.1. The main elements of this process will include:

- Identification of critical computer systems.
- Identification and prioritisation of key users/user areas.
- Agreement with users to identify disaster scenarios and what levels of disaster recovery are required.
- Identification of areas of greatest vulnerability based on risk assessment.
- Mitigation of risks by developing resilience.
- Developing, documenting and testing business continuity guides identifying tasks, agreeing responsibilities and defining priorities.

23.4. Planning framework

23.4.1. The Business Continuity guide will address the following levels of incident:

- Loss of key part of CMHS network.
- Loss of the CMHS primary server.

23.4.2. However, in the event of

- Loss of key user area within a building.
- Loss of a key building.

The Senior Management team and the IS&M Team will meet to identify the level of loss and course of action e.g. if the CMHS's server(s) become damaged and unusable following the loss of a key building, it will become necessary to relocate and/or purchase new equipment; set up the CMHS network and then apply the Business Continuity Guide in order to resume operation. See Appendix E, Asset/Information Loss.

23.4.3. The Business Continuity guide will include:

- Actions to be taken to get users of the CMHS network up and running again as soon as possible.
- Testing procedures describing how the Business Continuity guide will be tested.

See Appendix E, Asset/Information Loss and Appendix H, Business Continuity Guide.

24. Key Contacts:

Centre for Suicide Prevention and University of Manchester

Name	Title	Role
Professor Sir Louis Appleby Secretary: Mrs C Rayegan-Tafreshi 0161 275 0714	Director, Centre for Mental Health and Safety	Overall responsibility for data security for NCISH
Dr Pauline Turnbull 0161 275 0737	Project Director, The National Confidential Inquiry into Suicide and Safety in Mental Health	Responsibility for implementation of the policy
Mrs Rebecca Lowe 0161 275 0700	Information Governance Officer, The National Confidential Inquiry into Suicide and Safety in Mental Health	Day to day operational liaison with NCISH Research IT and Administration Manager on implementation and adherence to the policy; IG training for staff
IT Service desk 0161 306 5544 (or University internal ext. 65544) Mrs Michelle Clayton Ext. 7755949	Service Integration Manager, IT Services	IT Area Support Manager covering the Jean McFarlane Building.
Mr Alan Carter 0161 275 8111	Records Management, DP and FOI Office, Records Manager	Data Protection Guidance
Dr Alice Seabourne	Medical Director	Caldicott Guardian, Greater Manchester Mental Health NHS Foundation Trust

25. References:

Guide to the General Data Protection Regulation
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Records Management Code of Practice for Health and Social Care 2021
https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

Information Security Management: NHS Code of practice 2007

https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice

Confidentiality: NHS Code of Practice 2003.

https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

'Information: To share or not to share. The Information Governance Review' (2013),
https://www.gov.uk/government/publications/the-information-governance-review

NHS Digital General Guidance

https://webarchive.nationalarchives.gov.uk/20110426225301/http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/

https://digital.nhs.uk/services/data-access-request-service-dars/data-access-request-service-dars-process/data-access-request-service-dars-guidance-notes-on-security

Public Register of Data Controllers
https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

A Manual for Caldicott Guardians 2017. UK Caldicott Guardian Council.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

Original version of ISMP: Explanatory notes – Section 60 of the Health and Social Care Act 2001.
https://www.legislation.gov.uk/ukpga/2001/15/notes/division/4/5/1?view=plain

See also NHS Digital Guidance:
https://digital.nhs.uk/services/data-access-request-service-dars/data-access-request-service-dars-process/data-access-request-service-dars-guidance-notes-on-security

University of Manchester regulations and policies on use of email and internet access
https://www.itservices.manchester.ac.uk/aboutus/policy/.

University of Manchester policies on IG, Information Security and Intellectual Property including:

- https://www.itservices.manchester.ac.uk/aboutus/policy/
- https://www.itservices.manchester.ac.uk/wireless/

- Acceptable Use of IT Facilities and Services Standard Operating Procedure for Staff: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221

- Information Security Policy: https://documents.manchester.ac.uk/display.aspx?DocID=6525
- Intellectual Property Policy 2015: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=24420
- Authority to access and monitor University IT account holder communications and data: https://documents.manchester.ac.uk/DocuInfo.aspx?DocId=16278
- University guide to email and sensitive data:

  https://www.itservices.manchester.ac.uk/email/staffemail/safe/confidential/

  See also: https://documents.manchester.ac.uk/display.aspx?DocID=19942
- Advice on file encryption: https://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/file/
- General advice on encryption: https://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/

  See also:

  https://documents.manchester.ac.uk/display.aspx?DocID=19943
- Data handling: https://www.itservices.manchester.ac.uk/cybersecurity/data-handling/
- General advice on PC/laptop security: https://www.itservices.manchester.ac.uk/cybersecurity/

  See also: https://www.itservices.manchester.ac.uk/cybersecurity/advice/

  https://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/laptop/
- University guidance on reporting data protection incidents https://www.staffnet.manchester.ac.uk/igo/data-protection/report-data-protection-incident/
- University Standard Operating Procedure on Information Security and Data Protection Incident Reporting https://documents.manchester.ac.uk/display.aspx?DocID=15678

  https://www.staffnet.manchester.ac.uk/igo/data-protection/report-data-protection-incident/

Guidance on data security breach management. Information Commissioner's Office. https://ico.org.uk/for-organisations/report-a-breach/

Scottish Government Records Management: NHS Code of Practice (Scotland) version 2.1, 2012, https://www.gov.scot/publications/scottish-government-records-management-nhs-code-practice-scotland-version-2-1-january-2012/pages/0/