Trust Policy

University Hospitals Plymouth NHS Trust

Information Security Policy

Issue Date	Review Date	Version
May 2021	May 2022	6.1

Purpose

This policy defines information security protocols, procedures and controls to protect to a consistently high standard, all electronic information assets held on and processed by Trust systems, staff and contractors, from internal or external damage, either deliberately or accidentally.

Who should read this document?

All staff should familiarise themselves with this policy and its supporting policy documentation.

Key Messages

This policy will define the key roles and responsibilities in respect of managing the security of electronic and paper information held by the Trust.

Core accountabilities	
Owner	IM&T Chief Technology Officer, Information Security Officer
Review	IM&T Senior Management Team
Ratification	Senior Information Risk Owner
Dissemination (Raising Awareness)	All IM&T Staff
Compliance	IM&T Chief Technology Officer, Information Security Officer

Links to other policies and procedures

Information Governance Policy
IM&T Change Control Policy
System Suppliers Remote Access Application Form
Network Security Policy
Internet Use Policy
NHSmail Acceptable Use Policy
Telecommunications Policy
Various System Level Security Policies

Version History

1	July 2007	Initial Document
2	December 2007	Major review in line with ISO 27001 and IG Toolkit
3	March 2009	Reviewed and reformatted
4	January 2010	Reviewed and no changes made
5.1	March 2012	Revised and reformatted
5.2	May 2013	Minor amendment to job titles
5.3	February 2014	Minor amendment to job titles and Trust Documents
5.4	March 2015	Review and minor amendments
5.5	July 2015	Minor amendments to job titles and committee structure
5.6	August 2016	Minor amendments to name change of HSCIC to NHS Digital
6.0	January 2019	Added Electronic Storage and Transfer section
6.1	May 2021	Minor amendments and reference to NHSmail Acceptable Use Policy and N365 use.

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and

better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

Contents

1 Introduction

University Hospitals Plymouth NHS Trust acknowledges that information is a valuable asset; therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed and protected in the interest of all its stakeholders.

It is therefore of paramount importance to ensure that, information is efficiently managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

Personal health data is held by the Trust on the patient's behalf either electronically or in paper format so that their care can be delivered effectively.

The Trust is under an obligation to the individual to ensure that their personal information is:

- Recorded accurately
- Not modified or lost during storage or transfer
- Not disclosed to unauthorised individuals
- Made available when and where needed for its intended purpose
- Not processed for any other purpose other than intended

The Trust also depends on information systems for its business viability, using contract monitoring, financial, manpower, works, supplies and many departmental systems. The correct functioning of all these systems is critical to the efficient running of the organisation.

The security of information systems is therefore of fundamental importance to maintaining the continuity of health care provision and to preventing and minimising the impact of security incidents on the Trust. A secure information system enables sharing of information to the benefit of the individuals concerned and the organisation.

2 Purpose

The purpose of this Information Security Policy is to preserve:

Confidentiality

Access to data must be confined to those with specific authority to view the data.

Integrity

Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to specification.

Availability

Information must be available and delivered to the right person, at the time when it is needed.

It will establish and maintain the security and confidentiality of information assets, information systems, applications and networks.

Key legislation and standards in respect of Information Security are the:

- Data Protection Act (2018)
- General Data Protection Regulation (GDPR) (2018)
- Caldicott Reports
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health and Social Care Act (2000)
- NIS Regulations
- NHS Records Management Code of Practice for Health and Social Care 2016

As well as an obligation to the Trust, many staff are also bound by the Codes of Conduct of their respective professional bodies and should refer to their respective organisations for details of their guidelines.

Individual systems will be required to implement and meet Information Standard Notices (ISNs) published by NHS Digital and be compliant with any other applicable legislation and regulations.

3 Definitions

Information System

An information system is a combination of hardware, software, infrastructure and trained personnel organised to facilitate planning, control, coordination and decision making in an organisation.

Information Asset

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and used effectively.

Information Asset Owner

Information Asset Owners (IAO) are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they “own” and provide assurance to the SIRO on the security and use of those assets.

Information Asset Administrator

Information Asset Administrators (IAA) ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date.

4 Duties

Trust Board

It is the role of the Trust Board to define the Trust's policy in respect of Information Security, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Senior Information Risk Owner (SIRO)

The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board. The SIRO will also be the Director responsible for the Information Governance agenda. This role is undertaken by the Director of Corporate Business.

IM&T Senior Management Team

The IM&T Senior Management Team are responsible for review and approval of this policy.

Caldicott Guardian

The primary responsibility for the role of Caldicott Guardian is to safeguard and govern the uses made of patient information within the Trust and the transfer of patient identifiable information outside the Trust.

Head of IT Security

The Head of IT Security is the responsibility of the IM&T Chief Technology Officer and is responsible for production of and compliance with this policy.

IT Security Officer

The IT Security Officer is responsible for coordination of information technology and cyber security under the guidance of the IM&T Chief Technology Officer.

All Managers

Managers within the Trust are responsible for ensuring that the policy and its supporting standards are built into local processes and that there is ongoing compliance.

All Staff

All staff, whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these requirements on a day to day basis.

Information Governance Committee Structure

The Trust has designated authority to the Caldicott and Information Governance Assurance Committee (CIGAC), chaired by the SIRO, to monitor the implementation and oversee the compliance of Information Governance.

The Caldicott and Information Governance Assurance Committee provides Information Governance assurance to the Trust Board.

5 Information Security Training

Information Governance eLearning contains key information security principles and is part of mandatory training which all staff are expected to complete annually. All new staff complete IG training at induction.

The Information Governance team will provide on-going awareness of information governance matters via the Trust official communication network. The IM&T Service Desk regularly publish bulletins when there is an identified information security issue.

Key staff groups will be identified for further bespoke Information Security training using the NHS Digital online Data Security Awareness training. This training is also advertised in Trust's official communication briefing.

Through audit and compliance monitoring, some staff may be identified as requiring additional information security training.

6 Control of Information Assets

Every information asset, (be it hardware, software, application or data) will have a named Information Asset Owner who will have overall responsibility for the security of that asset.

Information Asset Administrators will be responsible for the day-to-day administration of the asset(s).

The IM&T Service will maintain an Information Asset Register, reviewed annually.

7 Electronic Storage and Transfer

In line with Department of Health and Social Care statements on a paperless NHS, where appropriate and viable, information shall be stored and transferred electronically using appropriate technology commensurate with the capabilities of the system (e.g. NHSmail, HL7 or SecureFTP).

Data-at-rest should be encrypted where it is not detrimental to the performance or operational characteristics of the system.

Electronic data transfers must be encrypted when traversing external networks or sent to individuals or organisations outside of the immediate Trust network.

Retention and disposal of electronic information should adhere to the NHS Records Management Code of Practice for Health and Social Care 2016 with records deleted in line with the retention schedule.

8 Access Controls

Staff are required to complete the IM&T Service Registration Authority process to receive a network account. Individual registration processes may exist for other information assets and systems.

Only authorised staff and third party contractors will be provided with access to information assets and information systems. Information Asset Owners will hold separate policies and registration processes where required and be responsible for ensuring authorised personnel have access only to areas appropriate to their business need. These policies will be defined in the System Level Security Policies.

Access to electronic information assets requires authentication via individual user account(s) or smartcards. Generic shared accounts should not be used as they lack audit and accountability.

Passwords are required to be strong, ideally where the system permits consisting of ten characters minimum, including at least one numeric or special character and a mixture of lower and uppercase. The information system should enforce password changes every 60-90 days if passwords are weak/short. Passwords can change every 365 days if they are deemed strong. Refer to “Why do we need complex Passwords?.pdf” Available via IT Help. Passwords must not be shared.

The responsible Information Asset Owner will manage and audit access to electronic and paper information assets.

Third party contractors or suppliers who have a business need to access information systems and assets are required to apply for access in accordance with the Trust Network Security policy.

Volunteers or other non-NHS staff requiring access to information systems are required to obtain an honorary contract prior to obtaining network access.

9 Electronic Software

Only software approved by the IM&T Service may be installed on Trust systems. Software will be installed by an approved Trust engineer or via the software management system Microsoft SCCM. Software purchased by the Trust remains the property of the Trust even when not installed and should never be transferred to non- Trust devices without prior written approval and transfer of license(s).

The IM&T Service are responsible for maintaining an effective compliance position in respects of software licensing. Where software is installed without a valid license it may be removed.

The IM&T Service will conduct regular software audits and usage will be monitored and metered to aid in identifying software which is not in use and can be recovered for redeployment.

10 Instant Messaging Software

In accordance with guidance published by NHS England (Nov 2018), instant messaging was recognised as a useful tool in supporting the delivery of direct care, particularly in

acute settings and during major incidents. WhatsApp, Viber, Telegram and Signal can be considered suitable, but the following should be considered:

- Minimise the amount of patient identifiable data you communicate
- Do not use instant messaging as a formal medical record
- Any advice received on instant messaging should be transcribed and attributed in the case note
- Instant messaging conversations may be subject to freedom of information requests or subject access requests
- Your device must require a passcode and lock out after a short period of inactivity
- Disable message notifications on your device's lock screen
- Ensure you have enabled any available remote-wipe features

Further guidance can be obtained from NHS England or your professional body.

11 Equipment Security and Controls

In order to minimise loss of or damage to assets, equipment will be physically protected from security threats and environmental hazards, based on risk assessments by the IAA.

Equipment assigned to individuals (e.g. laptop or mobile telephone) are the personal responsibility of that individual and all relevant precautions should be taken to ensure continued protection from data loss or theft. Individuals should not alter, modify or remove equipment in a manner which exposes information to data loss, theft or risk. Individuals must ensure that their equipment is kept up to date with the latest available software updates and patches.

Trust electronic information assets will be managed by the IM&T Service using appropriate systems and procedures and in accordance with the Network Security policy. A Configuration Asset Management Database of all electronic assets will be maintained in conjunction with an Information Asset Register which will be reviewed regularly for accuracy and completeness.

Mobile devices such as laptops, portable hard drives and smartphones will have either full disk encryption or encryption of data at rest.

Disposal of electronic information assets must be coordinated through the IM&T Service. In cases of hardware disposal, hard drives will be removed and destroyed according to the safe disposal procedure.

Personal devices may not be used for the storage, processing or transmission of business or person identifiable data. Certain removable storage devices defined by the IM&T Service, purchased privately, may be used if they meet security and encryption requirements which are available upon request.

12 Access to Network Services

Access to network services is restricted to Trust devices or third party systems where prior approval from the IM&T Service has been granted, in accordance with the Network Security Policy.

No personal devices are permitted to access the Trust network. The only exceptions to this rule is access provided by the private wireless networks 'NHS WiFi' and 'GovWiFi' and remote access to Citrix, where devices are segregated from the Trust network using appropriate security protocols.

13 Remote Access

Remote access requirements are detailed in the Network Security Policy.

14 Antivirus and Malware Protection

Antivirus and malware protection is the responsibility of the IM&T Service to configure, maintain and monitor. All Trust devices are required, where possible, to have Sophos antivirus and malware protection software installed. Any exceptions are agreed by the IM&T Service.

Devices which cannot be joined to the Windows network are required to have alternative precautions configured to protect against viruses and malware. Where on-device protection is not possible, the device(s) must be segregated from other devices on the network using firewall or access control list technology.

15 Removable Storage Devices and Media

All Trust devices, where possible, will have Sophos Endpoint Control software installed to restrict removable media devices allowing data to be written only to approved, secure products.

Removable storage devices must be encrypted to AES 256bit standards.

Confidential or person identifiable data written to CD or DVD must first be encrypted and the IM&T service can provide guidance on how best to do this.

16 Internet, Email and Cloud Storage

Use of the Internet is defined in the Internet Use Policy.

Use of email is defined in the NHSmail Acceptable Use Policy. Emails containing confidential or person identifiable data can be sent between NHSmail addresses, however email is not a clinical record and it should not be used as an archive.

Patient identifiable or confidential information can be sent from NHSmail to non-NHSmail addresses by using the encrypted [SECURE] email function. Guidance on usage is available on the IM&T intranet site, TechNET.

Under no circumstances should confidential or person identifiable data be uploaded to and stored within personal consumer or commercial cloud storage services (e.g. Dropbox or OneDrive). Use of these services is only permissible for anonymised data or publicly available documentation.

The OneDrive, Sharepoint and Teams components of the NHSmail Central Tenant N365 is approved for the exchange of clinical/sensitive data in line with the National Clinical Safety Case. N365 should not be used to store clinical information as it is not a safe or

approved electronic patient record solution. Clinical data created in N365 should always be moved to the main clinical record and any national data opt out considerations should be addressed in the clinical record repository.

17 Change Control

The IM&T Service conducts changes to electronic information assets in accordance with its Change Control Policy.

18 Assurance

Each system or collection of information assets which contain person identifiable data will have a nominated Information Asset Administrator (usually the system manager) responsible for the creation and on-going review of the System Level Security Policy (SLSP) and accompanying risk assessment. SLSPs will be reviewed annually.

19 Business Continuity and Disaster Recovery

The organisation will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks. It is the responsibility of system managers and/or Information Asset Owners to ensure that this is kept up to date, recorded in System Level Security Policies and revised annually.

20 Security Incidents

All security incidents and weaknesses relating to any information asset are to be reported to the IM&T Service Desk immediately and any compromise to patient safety, confidentiality or integrity of the clinical record should be reported on Datix and to the Information Governance Team.

Instances of virus outbreaks will require immediate isolation and removal from the network of infected devices or systems until the Trust can investigate and clean the infection.

Staff members that compromise the security of person identifiable information may be subject to disciplinary action in line with the Performance and Conduct Policy.

21 Overall Responsibility for the Document

The SIRO is responsible for ratifying this document. The IT Security Officer has responsibility for the review of this document.

22 Consultation and Ratification

The IM&T Senior Management Team has approved this policy and it has been ratified by the SIRO.

23 Dissemination and Implementation

Following approval and ratification this policy has been publicised across the Trust.

Publication of this policy has been publicised in the IG StaffNet Page, the Trust's weekly staff news briefing. All Departmental Heads have had the policy sent to them and the policy is available on Trust Documents.

24 Monitoring Compliance and Effectiveness

Compliance with this policy will be monitored by the completion of the Data Security and Protection Toolkit submission process. The evidence submitted for which is subject to annual audit.

Data Security and Protection Toolkit update reports will be presented by the Information Governance Team to the Caldicott and Information Governance Assurance Committee.

The Information Governance Team will monitor national and local developments that may affect this policy.

The IM&T Service will monitor installed software for applications which have been installed without prior authorisation or have the potential to introduce increased risk to data contained therein.

Changes to information systems will be audited and reviewed by the IM&T Service Change Advisory Board.

25 References and Associated Documentation

Data Protection Act 2018/General Data Protection Regulation and the

Freedom of Information Act 2000 (further information on the Information Commissioner's Office website – www.ico.org.uk)

Information Security Management: NHS Code of Practice
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/securitycode.pdf

Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk

Copyright, Designs and Patents Act (1988)
http://www.legislation.gov.uk/ukpga/1988/48/contents

Computer Misuse Act (1990) http://www.legislation.gov.uk/ukpga/1990/18/contents

Human Rights Act (1998) http://www.legislation.gov.uk/ukpga/1998/42/contents

Regulation of Investigatory Powers Act (2000)
http://www.legislation.gov.uk/ukpga/2000/23/contents

Information Security Management: NHS Code of Practice
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142

Instant Messaging https://digital.nhs.uk/binaries/content/assets/website-assets/data-and-information/ig-resources/information-governance-considerations-for-individuals-on-the-use-of-instant-messaging-software-in-acute-clinical-settings.pdf

Dissemination Plan and Review Checklist | Appendix 1

Dissemination Plan			
Document Title	Information Security Policy		
Date Finalised	May 2021		
Previous Documents			
Action to retrieve old copies	To be managed by the Document Controller		
Dissemination Plan			
Recipient(s)	**When**	**How**	**Responsibility**
All Trust staff	May 2021	IG StaffNet Page	Document Controller

Review Checklist		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
Content	Is the objective of the document clear?	Yes
	Is the target population clear and unambiguous?	Yes
	Are the intended outcomes described?	Yes
	Are the statements clear and unambiguous?	Yes
Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes
	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

Equalities and Human Rights Impact Assessment | Appendix 2

Core Information	
Date	May 2021
Title	Information Security Policy
What are the aims, objectives & projected outcomes?	The Information Security Policy will establish and maintain the security and confidentiality of information assets, information systems, applications and networks.
Scope of the assessment	
This assessment will highlight any areas of inequality with the implementation of this policy.	
Collecting data	
Race	This is mitigated as the policy can be made available in alternative languages.
Religion	The document has no impact in this area.
Disability	This is mitigated as the policy can be made available in alternative formats.
Sex	The document has no impact in this area.
Gender Identity	The document has no impact in this area.
Sexual Orientation	The document has no impact in this area.
Age	The document has no impact in this area.
Socio-Economic	The document has no impact in this area.
Human Rights	The document has no impact in this area.
What are the overall trends/patterns in the above data?	There are no trends/patterns in this data. External consideration has been given to 2011/12 NHS Litigation Authority Risk Management Standards for NHS Trusts, Care Quality Commission Outcomes and Information Governance Toolkit requirements.
Specific issues and data gaps that may need to be addressed through consultation or further research	Trust wide documents can be made available in a number of different formats and languages if requested. No further research is required as there are no further equality issues.

Involving and consulting stakeholders	
Internal involvement and consultation	This policy has been compiled by the IM&T Chief Technology Office and the IT Security Coordinator. The policy has been circulated for consultation to members of the IM&T Senior Management Team and the Caldicott and Information Governance Group.
External involvement and consultation	External consideration has been given to 2011/12 NHS Litigation Authority Risk Management Standards for NHS Trusts, Care Quality Commission Outcomes and Information Governance Toolkit requirements.
Impact Assessment	
Overall assessment and analysis of the evidence	This assessment has shown that there could be an impact on race or disability groups. However, this document can be made available in other formats and languages if requested. The document does not have the potential to cause unlawful discrimination. The document does not have any negative impact.

Action Plan

Action	Owner	Risks	Completion Date	Progress update
Provide document in alternative formats and languages if requested.	Information Governance Team	Potential cost impact.	Ongoing	This action will be addressed as and when the need occurs.