Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title

Title: Information Security Policy

Version: 5

Reference Number: CO11

Keywords:
Information, Security, Privacy, Confidentiality, Integrity, Availability,

Supersedes: V4
Description of Amendment(s):

- Inclusion of Privacy Impact Assessment (PIA) requirements

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Jenny Spiers

Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process
Equality Relevance Assessment Undertaken by: Information Risk Manager
ERA undertaken on: 2 March 2012
ERA approved by EIA Work group on: 23 April 2012

Where policy deemed relevant to equality-
EIA undertaken by N/A
EIA undertaken on N/A
EIA approved by EIA work group on N/A

Pennine Care NHS
NHS Foundation Trust

Approval and Ratification

Referred for approval by: Information Governance Manager

Date of Referral: 1st March 2017

Approved by: Information Governance Assurance Group

Approval Date: 1st March 2017

Date Ratified by Executive Directors: 20th March 2017

Executive Director Lead: Director of Service Development and Sustainability

Circulation

Issue Date: 23rd March 2017

Circulated by: Information Department

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? YES

Review

Review Date: March 2018

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 23rd March 2017

1. Introduction

This top-level information security policy is a key component of Pennine Care NHS Foundation Trust's (PCFT) overall information security management framework and should be considered alongside more detailed information security documentation including system level security policies, security guidance and protocols or procedures.

This document defines the Information Security policy for Pennine Care NHS Foundation Trust and applies to all business functions and covers all PCFT information, information systems, networks, applications, locations and users.

This Policy applies to all staff and contractors of Pennine Care NHS Foundation Trust and partner organisations who access the Trust information or information systems.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of PCFT's Information Security Policy are to preserve:

- **Confidentiality** - Access to data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available for the right person at the right time.

2.2. Policy aim

The aim of this policy is to establish and maintain the security, accessibility and Integrity of information, information systems, applications and networks owned or contracted to PCFT by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all PCFT information, information systems, networks, applications, locations and users of PCFT or supplied under contract to it including:

- Information collected, processed, stored and communicated by or on behalf of the Trust
- Software that is owned or operated by the Trust or is used for Trust business
- Websites and the internet when accessed via the Trust's network or when being used for Trust business
- The corporate network and servers that process Trust information whether located within or outside the Trust
- Any device that connects to the corporate servers and network or that accesses Trust information, including PCs, printers, laptops, other portable devices, memory sticks, smart phones, discs and tapes.

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Chief Executive of PCFT but on a day-to-day basis the Information Governance Manager and ICT Director shall be responsible for managing and implementing the policy and related procedures.

3.2. Line managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas;
- Their personal responsibilities for information security;
- How to access advice on information security matters – see 5.21 for contact details

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

All staff have a responsibility to only access clinical information they have a legitimate relationship with as part of their formal job role.

3.4. The Information Security Policy shall be maintained, reviewed and updated by the Information Governance Manager and ICT Director. This review shall take place every two years or when needed.

3.5. Line managers shall be individually responsible for maintaining the security of the physical environment where information is processed and stored.

3.6. Each member of staff shall be responsible for the operational security of the information systems they use and for reporting any problems they find in relation to the security of the system.

3.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality,

integrity and availability of the information they use are maintained to the highest standard.

3.8. Contracts that allow external contractors access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies. There may also be a requirement for an additional data sharing agreement to be in place.

4. Legislation

4.1. PCFT is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of PCFT who may be held personally accountable for any breaches of information security for which they may be held responsible. PCFT shall comply with the following legislation and other legislation as appropriate: -

- The Data Protection Act (1998);
- The Data Protection (Processing of Sensitive Personal Data) Order (2000);
- The Copyright, Designs and Patents Act (1988);
- The Computer Misuse Act (1990);
- The Health and Safety at Work Act (1974);
- Human Rights Act (1998);
- Regulation of Investigatory Powers Act (2000);
- Freedom of Information Act (2000);
- Health & Social Care Act (2012);
- The Protection of Freedoms Act (2012);

5. Policy Framework

5.1. Management of Security

- At board level, responsibility for Information Security shall reside with The Senior Information Risk Owner (SIRO)
- PCFT's Information Governance Manager and ICT Director shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. Information Security Awareness Training

- Information Governance awareness shall be included in the staff induction process, and Information Security shall form part of the annual mandatory IG training that all staff are required to complete.

- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a information security clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian (Information Assets Owner (IAO)) who shall be responsible for the information security of that asset.

5.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.8. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

5.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

5.10. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the relevant working groups or Executive Directors.

5.11. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of

their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded in accordance with the requirements of the Information Risk Policy. Action plans shall be put in place to effectively manage those risks. The risk and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Information Governance Manager or the Senior Information Risk and Governance Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.13. Protection from Malicious Software

PCFT shall use software counter-measures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on any Trust ICT asset without permission from ICT. Users breaching this requirement may be subject to disciplinary action.

5.14. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment; require the approval of the Information Governance Manager and ICT approval, before they may be used on PCFT's systems. Such media must also be fully virus checked before being used on PCFT's equipment. Users breaching this requirement may be subject to disciplinary action.

5.15. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts

- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

5.16. Accreditation of New Information Systems

PCFT will ensure that a Privacy Impact Assessment (PIA) is undertaken prior to the implementation of all new information systems, applications and networks to confirm the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements (See policy CO107 IG Requirements for New Processes and Systems for further information). PCFT has developed a series of System Level Security Protocols (SLSPs) for systems under its control in order to distinguish between the security management considerations and requirements of each. In this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system. A separate illustrative template is provided to aid the local development of these SLSPs at appendix 1.

5.17. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Information Governance Manager and ICT Director.

5.18. Business Continuity and Disaster Recovery Plans

PCFT shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

5.19. Reporting

The Senior Information Risk Owner (SIRO) shall keep the Board informed of the information security status of the organisation by means of an annual reports and presentations.

5.20. Policy Audit

This policy shall be subject to audit by the Audit Committee and External Auditors.

5.21. Further Information

Further information and advice on this policy can be obtained from The Information Governance Manager on 0161 7163145 or by emailing pcn-tr.ig@nhs.net

Pennine Care NHS
NHS Foundation Trust

Appendix 1
System Level Security Protocol

1. INTRODUCTION

The development, implementation and management of a system level security protocol will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

An effective a system level security protocol will therefore contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise) of person identifiable, sensitive or business critical data.

Where the system is available to multiple organisations, the system level security protocol must establish the necessary common policy, security parameters and operational framework for that system's expected operation including any functional limitations or data constraints applicable to one or more bodies.

The following series of topics are relevant for any system level security protocol and are intended to help guide responsible staff through their considerations for the development of their system level security documentation. This list is not exclusive of all possibilities and it is the responsibility of each information asset owner to identify and consider their security management needs on a case by case basis. This is best achieved through a formal process of risk assessment and mitigation.

Please liaise with IT services and System Contractors/Suppliers, where necessary to ensure that this procedure is completed.

2. SYSTEM DETAILS:

The System shall be known as: *[Insert full System Name]*	
The System's responsible information asset owner shall be: *[Insert details for the most senior member of staff accountable for the system i.e. Associate Director]*	Name: Job Title: Department: Extension:
The System's responsible information asset administrator shall be:	Name: Job Title: Department:

[Insert details for the member of staff responsible for the day to day management of the system i.e. System Manager] *(Note: this member of staff is the lead individual responsible for accrediting the system's security implementation)*	Extension:
The System's deputy information asset administrator shall be: *[Insert details for the member of staff who will deputise for the IAA in their absence]*	Name: Job Title: Department: Extension:
The Systems Data Controller shall be:	
What information is held on the system e.g. Demographics, Clinical Details	
Is the System compatible with the NHS Number? Yes/No	

3. SYSTEM SECURITY:

3.1 Security of the system shall be governed by Pennine Care NHS Foundation Trust's corporate information security policy and other associated policies and procedures.

3.2 The System shall incorporate the following security countermeasures:

Access Control: [logical security measures and privilege management]				
Authentication Method: *[Please tick]* *Access control must be in place on all systems. Authentication should ideally be by username & password or two factor authentication.*	User Name & Password:		Two Factor (Smartcard)	
	Other (Please Specify)		Two Factor (Other – Please Specify)	
Password Complexity: *[Note: If any of this criteria is not met, please identify this as a risk in the system risk assessment]* *The minimum password complexity should be:* *A minimum of 8 characters* *Require a combination of at least letters and numbers and ideally symbols.* *Require a mixture of UPPER and lower case characters.*	Maximum number of characters:		Minimum number of characters:	
	Minimum number of letters Required:		Minimum number of numbers Required:	
	Minimum number of lowercase characters required		Minimum number of uppercase characters required	
			Minimum number of symbols/special characters required:	
Password change period: Every…..				

Systems should force users to change their passwords at least every 3 months.	
Number of allowed password attempts before user account locked *Accounts should lock if a user enters an incorrect password 3 times. The user should then be required to contact a system administrator to re-activate their account (see un-lock procedure below).*	
If the system is accessed by username and password, does the system identify which element (i.e. username or password) that has been entered incorrectly? *(Yes/No)* *The system should not identify, which element has been entered incorrectly.*	
Un-lock Procedures: *(Please document how a user goes about retrieving their username/password if forgotten and/or unlocking their account)* *There should be a process in place to confirm the identity of the user prior to un-locking their account.*	
Inactivity time-out period: *Time out periods may vary considerably. Ideally the time-out period should be set to 10 minutes of inactivity.*	
Registration procedures: *[Note: Include procedures as an appendix if already established in a separate document. Please document any security/system training provided to users].* *All access provided should be authorised & users should be provided with appropriate system/security training.*	
Deregistration procedures: *[Please include a statement as to whether the IAA has access to leavers reports from the Human Resources department and how access is changed or removed for staff changing roles within the Trust].* *Please also include procedures for any temporary access/accounts given i.e. whether a termination date is set.* *All system manager's/IAA's should use ESR reports to deactivate system accounts that are no longer required. System managers should ensure, where temporary accounts are used, that they are appropriately 'timed' and/or removed when no longer required.*	
Records of all users and access levels provided are retained by the IAA: *Yes/No* *Records of all users and access provided should be retained by the system manager/IAA.*	
Please list all 'privileged users' of the system *i.e. users that can change core components of the system, including access levels, e.g. system administrators.* *Records of all users and access provided should be retained by the system manager/IAA*	

Please identify the possible levels of access *a user can be given and list any significant user groups. This may be job role specific or by user group.* *Records of all users and access provided should be retained by the system manager/IAA*	

Physical Security Controls for Hardware e.g. Server/s, back-up tape drives etc.: *Access control and security should be applied to all server rooms. Other hardware such as back-up tapes should be stored safely and securely i.e. in a physically secure area and fire proof safe.*			
Secure Room Yes/No		Secure Cabinet Yes/No	
Other (Please Specify)			

Network Security Controls: *The network should be protected by appropriate technical measures, such as firewalls, intrusion detection etc.*			
Firewalls Yes/No		Network Segregation Yes/No	
Other (Please Specify)			

Additional Security Controls: *All contractors should provide assurance of their compliance with information security requirements and best practice, by means of completing the IGT for third parties or providing an ISO27001 accreditation certificate.* *Penetration testing should be undertaken on the Trust's network at least annually. Individual servers may require a separate penetration test depending on the circumstances.* *All systems should log and retain audit trails i.e. log on audits, access to records and modification of records. A random sample should be selected from these audit trails and the appropriate checks undertaken to ensure records/systems have been accessed appropriately.*			
Contractor/Supplier Certification arrangements		Security testing i.e. Independent Penetration Testing	
Audit Trails (Please Specify e.g. Log on audit and whether/how this is checked/monitored)		Other (Please Specify)	

4. SYSTEM MANAGEMENT:

Maintenance & Support:	
The System shall be developed / provided by: *[Insert provider full Name]* (Note: if the system is developed or provided under commercial contract, then the relevant contract schedules that bind the contractor to the lead organisation's corporate security policy and to this system level security policy should be referenced)	
The System shall be implemented by:	

The System shall be maintained by: [Please note under what arrangements include responsibility for relevant aspects of security configurations. Also, identify the conditions applicable for the repair / replacement / disposal of equipment or media that may contain person identifiable data]. Equipment must always be handled and destroyed securely. Where equipment is no longer required an appropriate certificate should be provided to evidence that equipment has been destroyed securely. An appropriate confidential agreement should be completed (signed by the IAO and the Contractor/Supplier) for reference. A risk assessment should be carried out prior to any proposed agreement with a third party, the risk assessment should as a minimum take into consideration the level of access and any use of sub-contractors.	
Remote Access Support Arrangements (if applicable): Please state whether the Contractor/Supplier requires remote access to the system and the arrangements in place to secure any personal data. Please state the method of access i.e. internet (WebEx), N3, VPN. Please reference any Remote Access Support arrangements within the Contractor/Supplier confidentiality agreement. Please refer to the Remote Access and Mobile Working Policy.	
The System shall be shared or used by the following organisations: (Note: record all participating bodies (stating whether NHS or other) and their purposes - Where the system is shared across multiple legal entities it is essential to identify how this security procedure will apply to all parties and how its effect will be measurable). An appropriate information sharing protocol and information sharing agreement should be completed for each organisation. Please refer to the Information Sharing Policy.	

5. SYSTEM DESIGN:

The System shall comprise **You may wish to delete the column which does not apply.**		
Electronic Based Systems:		**Paper Based Systems:** [Please describe the elements of the system. It maybe useful to use a flowchart. Please put as an appendix if necessary].
Describe the system and purpose.		
Describe the local network that will house the system i.e. existing Trust network or independent network?		
Does the system require the use of a dedicated/virtual file server? Please state.		
Does the data reside with the system software? Please state where the data resides i.e. server/ network drive.		
State any links to any wider network clouds e.g. site LAN, Internet and / or any other external network		
State any firewalls / gateway control devices.		

6. OPERATIONAL PROCESSES:

Back-Up Procedures:	
Back-Up Routine: [Please identify the frequency back-up data is recorded. Please specify arrangements for both system data and software]. System data should be backed up at least on a daily basis. System software should be backed up at least weekly.	
Verification Routine: [Please identify and data validity tests undertaken]. *All back-ups should be verified / validity test undertaken daily.*	
Shutdown/Restart Process:	
Dependencies:	

[Please identify any interfaces the system has in place e.g. to PAS].	
Testing: [Please identify the frequency of tests, whether test data is used, whether tested in a simulated live environment and by what means the test is undertake, for example simulations/walk through exercises]. *Back-ups and recovery plans should be tested regularly (at least annually). Table top exercises should be undertaken using test data in a simulated live environment i.e. using back-up servers.*	

Collection Activities:	
The person identifiable / sensitive data will be collected by: [Please Tick].	
Directly from the Data Subject e.g. the patient is present when providing the information and the information is directly input on the system.	
On-line means i.e. Internet/Intranet/Email: [Please indicate security arrangements e.g. SSL VPN and encryption standards]. Encryption must meet approved NHS standards i.e. 256 bit strength.	
Paperwork**:** [Please indicate security arrangements e.g. follow-up arrangements to identify lost post for posted paperwork]. Safe Haven procedures must be followed. Please see the Information Sharing Policy.	
Data on CD: [Please indicate security arrangements e.g. encryption standards]. Encryption must meet approved NHS standards i.e. 256 bit strength.	

Storage Arrangements:	
The data will be stored: [Please Tick]	
In what format (paper or electronic), where will it be stored & under what security controls?	
Any anonymisation process for person identifiable / sensitive data will need to be described. Please state whether data is pseudonymised for all secondary purposes? If not please identify which secondary purposes use identifiable information.	
How (and under what security controls) will person identifiable / sensitive data be loaded onto any file server / storage device.	
Encryption standards should be employed for stored data. (Note: any device not in a secure area that will cache or store person identifiable / sensitive data needs to do so on an encrypted drive, or within an encrypted container. Backup copies of person identifiable / sensitive data also need to be encrypted). Note: for added risk protection staff are encouraged to encrypt person identifiable / sensitive data stored on devices located in secure areas. Although not an NHS requirement, it may be prudent that such a step is taken should it be perceived a possibility of equipment loss or other attack.	

Processing Arrangements: **You may wish to delete the column which does not apply.**

The data will be processed: [Please Tick]		
Electronic Based Systems:		**Paper Based Systems:** [Please describe the elements of the system. It maybe useful to use a flowchart. Please put as an appendix if necessary].
List the user devices (desktop, laptop, PDA, etc) that will access and process the data.		
State whether any of these devices will cache or store any of the data. If so, indicate the encryption standards to be employed. (Note: any device not in a secure area that will cache or store person identifiable / sensitive data needs to do so on an encrypted drive, or within an encrypted container).		
State whether remote access (over the Internet or otherwise) will be employed to access the data.		
Describe measures in place to prevent the interception of transmitted data (E.g. standalone network, encrypted path, etc).		
Include any policy to prevent (or at the very least severely restrict) the copying of person identifiable / sensitive data to removable media.		
If applicable, include any policy to prevent the printing of person identifiable / sensitive data.		

Peripherals:				
Sufficient stock of any hardware required for the system is available at all times i.e. Smartcards / digital microphones. Please detail all available stock.				
Any spare stock is stored securely	Secure Room Yes/No		Secure Cabinet Yes/No	
	Other (Please Specify)			

Disposal Arrangements:
When the system or its data has completed its purpose / has become redundant

or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data: (Note: that operating system provided utilities such as 'erase' may not destroy unwanted data – it is therefore desirable to employ a commercial strength data shredder or equivalent to prevent unauthorised disclosure of person identifiable / sensitive data).

7. SYSTEM AUDIT:

7.1 The System shall be risk assessed every 12 months by applying Pennine Care NHS Foundation Trust's risk assessment method.

7.2 A risk management / security improvement plan shall be established to address all unacceptable risks.

Note:

i) Remember to take account of cross-boundary risk / dependency issues where the system is part of a larger service or multiple organisation arrangement.

Audit Arrangements:
The System shall benefit from the following internal / external audit arrangements (Please list all arrangements).

8. SYSTEM PROTECTION:

Business Continuity Plans:	
Business impact Review: *[Briefly explain/analyse the effect that a disruption might have upon your/the Trust's business function].*	
Disaster recovery arrangements: [Explain what resilience / contingency arrangements the system benefits from	

e.g. uninterrupted power supply (UPS)]. (Note: identify any separate plans and status).	
Planning: In the event of serious disruption or total system failure, business continuity shall be provided by the following means:	
Confidentiality: In the event of a security or confidentiality breach occurring the following procedure shall be followed:	

Malicious Code / Unauthorised Mobile Code:	
What controls and procedures are in place to protect against malicious code and unauthorised mobile code i.e. anti-virus software [Please specify the software name].	
Does the system support security updates to the server operating system? Yes/No	