University Hospitals of Leicester NHS
NHS Trust

Control of Access to Electronic Systems UHL Policy

Approved By:	Policy and Guideline Committee
Date Approved:	**19 June 2007**
Trust Reference:	**B25/2007**
Version:	2
Previous version:	1.4 June 2016 Policy and Guideline Committee
Author / Originator(s):	IM&T Head of Design Authority – Infrastructure
Name of Responsible Committee/Individual:	Chief Information Officer
Latest Review Date	17 July 2020 – Policy and Guideline Committee
Next Review Date:	February 2024

CONTENTS

Section		Page
1	Introduction	3
2	Policy Scope- Who The Policy Refers To And Specific Exemptions	3
3	Definitions and Abbreviations	4
4	Roles – Who Does What	5
5	Policy Statements and Associated Documents-What needs to be done	6
6	Education and Training	14
7	Process for Monitoring Compliance	15
8	Equality Impact Assessment	16
9	Supporting References, Evidence Base and Related Policies	16
10	Process for Version Control, Document Archiving and Review	16

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

Revision History

2007	V1.0	Original prepared by IM&T Security Manager
April 2009	V1.1	Prepared document using original unapproved version 1
Aug 2009	V1.2	Used standard document template
Dec 2009	V1.3	Modified to comply with PGC recommendations
Nov 2015	V1.4	Reviewed & updated
June 2020	V1.5	Reviewed & updated password length

KEY WORDS

Access to electronic systems

Access to computer systems

Login to computer

Authentication

1 INTRODUCTION

The control of access to electronic data is deemed to be highly important by the NHS; failure to manage secure access to data can result in a large fine from the Information Commissioners office (I.C.O.) and adverse reputational impact on any organisation failing to comply with these standards.

UHL is mandated to use the standards set out by the NHS to control access to data stored on electronic (computer) systems, thus mitigating any risk of unauthorised access to data stored on UHL electronic computer systems.

The aim of the standards is to control access to sensitive data and furthermore to offer assurance to stakeholders (includes patients, relatives etc.) that their personal details are being maintained and stored in a secure, safe manner.

This policy provides assurance to the following requirements laid out by NHS Digital to comply with the Cyber Essentials Plus requirements –

The standards detailed in this policy are mandatory and are derived from mandatory NHS Digital security standards.

Compliance with this policy is submitted as evidence to the NHS Information reporting via DS&P (Data Security & Protection) toolkit and that will feed into CE+ (Cyber Essentials Plus), a mechanism used by the NHS to ensure best practice is being used to securely manage information

The management of data is summarised in the following statement from the UHL privacy board:

Confidentiality – ensuring that sensitive and/or business critical information is appropriately protected from unauthorised 3rd parties and can only be accessed by those with an approved need to access that information

Integrity – ensuring that information has not been corrupted, falsely altered or otherwise changed such that it can no longer be relied upon

Availability – ensuring that information is available at point of need to those authorised to access that information

2 POLICY SCOPE

This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures for the control of access to electronic systems which contain sensitive data, in particular patient identifiable data (P.I.D.)

This Policy applies to all users of electronic information to include:

- Trust employees
- Honorary trust members
- Employees of temporary employment agencies

- Medical and nursing students

- Vendors, business partners, contractor personnel and functional units regardless of geographic location.

- This policy applies to all systems designed to hold data electronically, owned by the Trust or entrusted to the Trust by internal and/or external customers these systems include, but are not limited to, computer systems (hardware, software and data), analysers and imaging equipment. The intended audience for this policy are primarily those responsible for establishing and maintaining access control systems. The policy reiterates user's responsibility not to share passwords and log in credentials with others.

3 DEFINITIONS AND ABBREVIATIONS

ACL (Access Control list) is a list of users which is presented as a group, authorised to access specific electronic data. This is a common technique used in systems management to handle large numbers of people accessing data, group membership grants access to data which would otherwise be denied to unauthorised users.

Access control system is a method of securing access to electronic data stored on a computer system, a system user is authorised to access data using the rules specified in the Access Control System

Active Directory is a directory based architecture provided by Microsoft to manage the components of a diverse network such as the one used at UHL, this allows the granular management of access control to thousands of personal computers and servers.

Authentication is the correct verification of an end user by virtue of a login name and password or a smart card and pin number

Authorisation is the allocation of access to electronic data dependant on successful authentication, usually by group membership after login is successful to the relevant computer system

Electronic Systems are essentially computer based technologies which can be as diverse as database servers, personal computers, analysers or tablet devices.

Generic User is a term used to describe an anonymous person who shares a login identity to access a system; these are frequently used in areas where login times are excessive and may adversely affect patient care. The use of Generic logins are no longer supported as they represent a threat to secure access of data, access is anonymous therefore the user cannot be verified

Information Asset Administrator (IAA) is someone within the organisation who manages a computer system containing data, both hardware & software can be considered an information asset. At UHL the Information Asset Administrator would normally be the IAA of one or more systems.

Information Asset Owner (IAO) is someone within the organisation who is responsible for the overall management of the information assets used by their part of the business, in UHL this would typically be the head of a division or department

Senior Information Risk Owner (SIRO) is someone designated to:

- Ensure organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist.
- Be responsible to Lead and foster a culture that values, protects and uses information
- Own the organisation's overall information risk policy and risk assessment process, test its outcome, and ensure it is used

Single-factor authentication is the traditional security process that requires a user name and password before granting access to the user, this can also be a smart card as used for single sign-on.

Two factor authentication, requires the user to provide dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code

4 ROLES- WHO DOES WHAT

4.1. Responsibilities within the Organisation

Senior Information risk Owner (SIRO) will:

- Advise the Chief Executive or relevant accounting officer on the Information risk aspects of his/her Statement of Internal Control

- Own the organisation's information incident management framework

(Currently the Chief Information Officer is the SIRO at UHL)

Information Asset Owners (IAO) must ensure that the requirements of this policy are adhered to at all times.

Information Asset Administrators (IAA) must ensure that the requirements of this policy are applied at all times and report any breach to the Information Asset Owner.

Chief Information Officer (CIO.) will develop and implement relevant security and information policies in line with statutory requirements; in particular but not limited to compliance with NHS information Governance Standards (IG Toolkit).

Managed business Partner (MBP) is responsible for implementing the policies and guidelines created by UHL and to report any identified breach using the formal procedures set out in the MBP contract to UHL IM&T management.

End users must comply with the requirements of this policy and any other policies which exist to ensure the security and confidentiality of electronic data.

4.2. Responsibilities of and communication with stakeholders

No access control system may be deployed without UHL IM&T approval.

The IM&T Design Authority will define Security standards to be implemented for all operating system, networks, applications and remote access based on the sensitivity of the data being accessed

It is the responsibility of the person using an information system (or their Manager) to inform IM&T and the Information Asset Owner that the person no longer requires access to that system for whatever reason.

It is the responsibility of the Manager of any person using an information system to inform IM&T and the systems Information Asset Owner that the person will not require access to a system due to extended absence e.g. maternity leave, sabbatical etc..

5 POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS

5.1. User Identification, Authentication and Accountability

Access to electronic information must be restricted to authorised users and must be protected by appropriate physical and logical authentication and authorisation controls. Protection for electronic information must be commensurate with the sensitivity of the information held, it may be necessary to use multi factor authentication in certain circumstances to achieve this aim.

Definitions:

- **User Identification**: A username provided to identify a user on a computer system.
- **Authentication**: The recognition of a user identity by the use of the correct password.
- **Accountability**: Is an essential part of an **information security plan**. The phrase means that every individual who works with an information system should have specific responsibilities for information assurance

Wherever possible the use of ACLs (Access Control Lists) will be used to control and manage access to electronic systems and data stored thereon.

The access control requirements for smartcards and their administration are defined by NHS digital and fall outside the scope of this policy, those requirements are however additional and do not conflict with the scope of this document.

5.2. Minimum Access Criteria

All systems used to access electronic information require a minimum of single factor authentication (e.g. username and password, Smart card & PIN, software token & PIN etc.)

The username may be displayed in clear on the login screen but the password must be masked.

- The login screen should not display the last user name entered.
- The password must be a minimum of fifteen characters
- The password will have a maximum lifetime of 365 days.

When a password expires or a change is required users should create a new password that is not identical to last ten passwords previously employed.

The password must be complex in nature and should consist of any mixture of alpha/numeric characters together with other special characters e.g. *+-&£$ etc.

The system must force the user to set their own password on first login to the system

The user must be able to change their own password at any time

A minimum of twelve months password history must be maintained on the system. Passwords stored electronically may not be stored in readable form where unauthorized persons might discover them.

Users will not be allowed to repeat the use of the same password for the last 10 passwords.

- A maximum of five successive login failures shall result in a user's account being locked out
- Automatic re-enablement of locked out accounts after a period of time will not be allowed, all password resets will be performed manually by the IM&T service desk on request.
- Passwords shall not be written down or left in a place where unauthorized persons might discover them.
- Passwords may never be shared or revealed to anyone other than the authorized user.
- If a password is suspected of being disclosed or known to have been disclosed to anyone other than the authorized user, it should be changed immediately.

5.3. Password Requirements-Guidance

Passwords provide a valuable role in protecting systems from unauthorised access and most effective when they:

- Have meaning
- Are not names and have no connections to the user

- Are changed every 12 months (or sooner if compromised) and are not related to: previous passwords, are NOT written down, are kept secret and divulged to no-one (this includes IT staff)
- Are NOT easily guessed, e.g. not VISITOR, GUEST, PASSWORD or similar
- Are NOT shared with any other individual

Effective password complexity can be achieved through a series of actions that prove impossible for another to decipher but remains memorable to the user. To further define this, a simple set of words that relates directly by association can be placed in effect. The words 'cheese trap mouse' is a suitable example. This means very little to any other staff member and is a satisfactory password combining letters. Passwords must be a minimum of fifteen characters.

Password complexity is automatically enforced by most systems accessed within the organisation. Where this is not the case, for example when changing passwords for access to third-party or some internally developed applications, those passwords used must be:

- A minimum of 15 characters e.g. which form into three words, unrelated to each other.

- When a new account has been created, the user must contact the IT Helpdesk to have it activated. Proof of identification will be required by the user when placing the call. An initial random password will be provided and the user will be forced to change as soon as they have logged on.

Only the person to whom the username and password have been issued are permitted to use those details to log on to a system. Use of usernames and passwords by people other than those to whom they have been issued will be treated as a serious lapse in security and could lead to disciplinary action.

Staff must **NEVER** divulge their passwords to anyone else, **including members of the IT Department**. Failure to keep passwords secret will be treated as a serious lapse in security and could lead to disciplinary action.

Staff leaving their workstations unattended must ensure that other members of staff cannot access their systems. They can either logout of their machines or lock them until they return. This is done by pressing CTRL-ALT-DELETE and selecting lock computer or log off. On some older systems, staff may only be able to log out using start -> log off. Systems can also be locked by holding the windows key and L. Leaving a computer unattended without locking access to that computer in the manner stated above could lead to disciplinary action.

If a member of the IT Department requires access to a workstation, it is the responsibility of the member of staff using the PC, their Manager or a responsible person designated by their Manager to be present during any work carried out.

In order to confirm the identity of a caller, the Helpdesk or other IT Departmental staff will ask for certain parts of a 'shared secret'. The 'shared secret' is a pass phrase previously provided by the user for use under such circumstances. The IT Department has access to a system which will randomly select certain letters from

the pass phrase (e.g. first, third and fourth) and will ask the caller to provide these before making security sensitive system changes such as password resets or file permissions amendments. In the event that a user is unable to accurately provide this information, an email from their Line Manager may be required before any such changes may be made. This procedure may be bypassed under exceptional circumstances in line with the extraordinary discretionary access section of this policy.

5.4. Password Resets

Password resets will be issued by the IM&T service desk to the UHL Email address of the requester by default, unless Email access is unavailable, in which case additional questions to validate authenticity of the requester may be posed.

Where possible the self-service password reset function available in the single sign-on facility (Imprivata) should be used to reset Active Directory / Windows passwords by end users.

5.5. User Access Privilege and Entitlement

It is a prerequisite of this policy, that anyone granted access to electronic systems has been through the appropriate personnel checks before employment / access is granted (Registration Authority as used for Smart Cards is acceptable).

Users who use their access for purposes which are not required by the Trust (e.g. looking up medical or demographic details of friends or family) (where personal information is concerned) are in breach of the Data Protection Act (1998) and the UHL Information Governance Policy (B4/2004)

5.6. Account Security

Users must never share their personal login credentials (including Smart cards & tokens) with anyone else for whatever reason. If a user inadvertently discloses their password then they should change it as soon as possible.

5.7. Generic logins

Requests for generic logins will no longer be approved as their use constitutes a risk to confidentiality as the user cannot be verified, Any generic logins found in use will be de-activated, users will be expected to use their own credentials to access systems and data, anyone experiencing difficulty with speed of access should contact IM&T to use the Imprivata single sign-on solution with their smartcard.

5.8. Access Termination, Modification or Revocation

Information Asset Owners are responsible for producing detailed processes for terminating, modifying or revoking user access.

Accounts must only remain active whilst they are required.

Accounts must be disabled as soon as a person leaves employment with the Trust.

Under no circumstances must an account be used by another person, either temporarily or permanently.

IM&T will monitor accounts for usage; any account not used for 90 days will be disabled for a further 180 days after which it will be scheduled for deletion.

Audit activity of account management is required to be maintained for 6 years after the individual has left the employment of the Trust (in line with the retention requirements for smartcards administration)

When an employee of UHL leaves the Trust a notification is sent by the ESR (NHS electronic Staff Record) to IM&T, thereby initiating the process of de-activating their user account.

5.9. Third Party Access

All third party access (contractors, business partners, consultants, vendors) must be appropriately authorised and monitored for compliance.

Third party access to electronic information will be granted for the minimum period necessary with a termination date set on the relevant account (this would normally be the end of contract date).

In cases where third party access is needed for long periods to satisfy service level agreements under support arrangements, the Information Asset owner must specify access timeframes and justification for such access. Where possible restrictions should apply to these accounts by disabling access until requested, this will prevent unauthorised changes being made to live systems.

5.10. Remote access for external suppliers shall also incorporate the following features:

Any account provided for external support shall be disabled until access is formally requested via service desk protocols

All requests for remote access shall be recorded by the service desk

The account will be disabled as soon as the external support session is completed.

The account shall not be left enabled for extended periods of time.

5.11. Access privileges

Access privileges must be authorised & revoked by the appropriate Information Asset Owner

Annual checks shall be performed by the MBP (Managed Business Partner) to prevent users gaining excessive rights when they move roles within the Trust.

Access to systems should be authorised on a need to use basis i.e. an individual should not be granted access in excess of that, which is required to fulfil their role within the Trust.

Where account holders are transferred to private companies e.g. when a service transfers under T.U.P.E. then access to UHL systems can continue, however transfer of data to third parties must be approved by the relevant Information Asset Owner from UHL.

Where access to UHL systems is required by third parties then the relevant Information Asset Owner from UHL should authorise access

5.12. Clear Screen Policy

Workstations will require entry of a valid username and password before the software installed on it or resources it provides may be accessed.

A Trust approved, non-changeable screen saver will be placed on PCs with a time out of between 10 minutes and 30 minutes, depending on location. This will be enforced from the Trust core systems and will not be changeable by staff. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action

5.13. Process for Monitoring Compliance

Staff are expected to comply with the requirements set out within the Password Management Policy and related policies. Compliance will be monitored via Manager and Information Governance Team reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the Information Governance Toolkit.

Non-adherence to the Password Management Policy and related policies will result in local disciplinary policies being implemented.

5.14. Provision for Extraordinary Discretionary Access to User Data

In exceptional circumstances and with full agreement of a member of the relevant individual's senior management team, access to another member's data may be facilitated by the IT Department.

This will normally be done by providing account logon details to the aforementioned manager if authorisation is given, in writing or via email, by any of the following:

- IT management lead (Chief Information Officer)
- Head of Privacy
- Caldicott Guardian

- HR

This information will be passed to an IT Department member of staff holding the necessary system privileges. The current password will then be reset to a new password for another person to access data held on the Trust systems.

6. EDUCATION AND TRAINING REQUIREMENTS

Information governance training is mandatory for all UHL employees, training materials can be found on the7 UHL training website at https://www.euhl.nhs.uk

7. PROCESS FOR MONITORING COMPLIANCE

POLICY MONITORING TABLE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements	Lead(s) for acting on recommendations	Change in practice and lessons to be shared
Compliance with this policy	Internal Audit	Random Audit of implemented controls	Annually	UHL Audit Committee	UHL Chief Information Officer	Change in policy if necessary
Access control processes to be monitored to detect non-compliance	Privacy Manager	Information security risk assessment	Monitoring results must be reviewed on a regular basis as determined by the information asset risk classification	Information asset owners are responsible for monitoring their access control processes to detect non-compliance with this Access Control Policy and to record evidence in case of security incidents.	Privacy Manager / IM&T Security Officer	Change in policy or processes if deemed necessary

8. EQUALITY IMPACT ASSESSMENT

Name of Policy / guidance Document: POLICY FOR THE CONTROL OF ACCESS TO ELECTRONIC SYSTEMS

The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9. SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

Principles of information security, Data Security & Information governance

Related Policies

- UHL Information Security Policy. Trust Ref A10/2003
- UHL Data Network Security policy, Trust Ref B48/2009
- UHL Firewall Policy

10. PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

Once this Policy has been approved by the UHL P&G Committee, Trust Administration will allocate the appropriate Trust Reference number for version control purposes.

The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts SharePoint system.

This Policy will be reviewed every three years and it is the responsibility of the Policy and Guideline Committee to commission the review

Contacts & Assistance

For information and guidance on the implementation of this policy, contact:

- The IM&T Service Desk on 8000
- The Chief Information Officer on 5391
- The Head of Privacy on 6053