Appendix B

University Hospitals Birmingham NHS Foundation Trust

Access Control for Specified Systems

Name of System:	
Name of authorising person:	
Job titles of authorising person:	

In accordance with the Caldicott Principle to ensure that access to patient confidential information is on a strict need-to-know basis, the Trust employs least privilege access controls to all systems. It is imperative that every system - whether accessed via local desktop PCs, communication networks and equipment, or larger systems machinery - contains appropriate mechanisms for ensuring that only authorised users may gain access to information, programs, files and databases.

Every system must be able to identify any user who justifiably requests access to it and repel all unauthorised intrusion, whether accidental or malicious. Equally, every system must ensure that even authorised users are only given access to those areas which they require in order to complete their working duties. Much of this control will be maintained by the use of user accounts and passwords. In addition, there must be a robust mechanism for ensuring that staff who leave the organisation no longer have access to the particular system and that staff who change position within the organisation only retain access to systems which are appropriate for their new job role.

The Trust recognises the value of information contained within their computer systems and will not tolerate unauthorised use. It is a criminal offence for an unauthorised person to attempt to access a system or information within systems or to attempt to exceed the computer facilities and privileges granted to them and the Trust will prosecute those committing any such offence as covered by the Computer Misuse Act 1990.

An authorising person must be identified for the system and they must be responsible for ensuring that access to the system is appropriate in accordance with the Caldicott Principles and the Data Protection Act 1998. This can be done by requiring staff to complete the attached form stating the reason for their request to access the system and their acceptance of the policies, procedures and laws relating to access to the information.

The authorising person must put in place a procedure to ensure that when a member of staff with access to the system changes position in the organisation, there is a local process to check if they still need access to the system. As an added safeguard, the authorising person must also review the list of approved users on a quarterly basis to ensure that the staff still require access to the system.

University Hospitals Birmingham NHS Foundation Trust

Request for Access

Name of System:	

I confirm that I have read and understood the following information:

1. I have attended mandatory Trust Information Governance annual training
2. I am aware that access to this system must be undertaken in accordance with Trust policies and procedures, including but not limited to the Data Protections & Confidentiality Policy, the Information Governance Policy and the Information Security Policy.
3. I am aware that access to this system must be undertaken in line with the Caldicott Principles, particularly the fourth principle that access to information is on a strict need-to-know basis. I will therefore only access confidential information where I am either directly involved in the healthcare of the person or have a legitimate purpose for work.
4. I will not share my access passwords for the system with any other person.
5. I understand that as an NHS employee, I have a legal duty of confidentiality.
6. I will report any suspected or known breaches of information security, or identified weaknesses within this system to the authorising person.
7. I will inform the authorising person when I leave the Trust or when I change employment role within the Trust.

Name			
Job Title			
Signature		**Date**	
Reason access is requested			
Name of authorising person			
Job title of authorising person			
Date approval for access is given			