NIHR | BioResource

NIHR BioResource

Information Governance (IG) Policy

Version 4.0

24 June 2021

A. Document Purpose

(A): This document details the high-level Information Governance (IG) Principles that form the policy for all staff and partners of the National Institute for Health Research (NIHR) BioResource for Translational Research (NIHR-BR).

The NIHR-BR aims to meet the information governance and security requirements required by the NHS, and completes the NHS Digital Data Protection and Security Toolkit (https://www.dsptoolkit.nhs.uk/), an annual self-assessment, auditable by NHS Digital.

(B): The entity for these studies is the NIHR BioResource for Translational Research, commissioned by NIHR and managed jointly by University of Cambridge and Cambridge University Hospitals NHS Foundation Trust.

(C): Cambridge University Hospitals NHS Foundation Trust (CUH) is the legal entity responsible for information governance, jointly with the University of Cambridge for the Rare Diseases part of the research activities.

(D): Scope – the Information Governance Policies apply to the information and operations supporting the collection of identifiable health-related and personal data for participants engaged in research studies, and to de-identified (also called de-personalised) participant data. As the document is under continuous review, resolved comments are permitted in an approved document to show the direction of travel.

(E): The policies do not apply to the data sets and services that relate to other business needs, e.g. finance and HR, which are managed within the governance framework supplied by the grant holder and primary employer, the University of Cambridge.

(F): Remit - The NIHR-BR supports several different programmes and each of these also have responsibility for their own Information Governance activities. Typically, this translates to the NIHR-BR service having responsibility for centralised electronic and paper records and the separate studies and projects have their own responsibility for the paper and/or electronic files at source.

(G): Responsibility and jurisdiction: Staff are employed by a number of organisations to provide this service. In many cases, their parent legal entity and /or employment contract stipulates compliance and method of working. The policies described in this document are the master policies which pertain to this work but are supported by the institutional policies where applicable. Where these policies have a specific bearing on this work, they are explicitly referenced e.g. IG training.

1 Management

1.1 Executive - Management Structure

1.1.1 The NIHR BioResource for Translational Research (NIHR-BR) is an infrastructure, funded by the NIHR. It has an Oversight Board answerable to the UK Government's Department of Health and Social Care; a Steering Committee under that, comprised of scientific representatives of all the NIHR-funded regional BioResource Centres and initiatives, plus other major stakeholders; and under that an Operational Management Group (NIHR-BR OMG). The frequency of meetings is 6-monthly, quarterly and fortnightly respectively. Information Governance is provided by Cambridge University Hospitals NHS Foundation Trust (CUH) and, where necessary, also by the University of Cambridge.

1.2 Executive - Management Commitment

1.2.1 The NIHR-BR Senior Management Team actively support information security within NIHR-BR through clear direction, demonstrated commitment, explicit assignment and acknowledgement of their – and everyone else's - information security responsibilities.

1.2.2 The NIHR-BR OMG has, in approving this Information Security Management System (ISMS) and the information security policy, expressed clear support for information security and ensured that the information security policy meets identified information security risks and supports the business goals.

1.2.3 The NIHR-BR OMG have explicitly assigned lead responsibility for information security in the management team to the Information Governance Responsible Officer (IGRO).

1.2.4 The NIHR-BR OMG has allocated clear responsibilities to management and specific individuals for specific aspects of information security and these responsibilities are documented throughout the ISMS.

1.2.5 The NIHR-BR OMG has ensured that there are adequate resources to provide the level of information security it requires.

1.2.6 The NIHR-BR OMG, in acknowledging that it is not a legal entity, has sought and gained the oversight of the Information Governance team at Cambridge University Hospitals NHS Foundation Trust.

1.3 Executive - Security Policy

1.3.1 This policy specifies management's intent to protect electronic information assets (e.g. data, systems) within NIHR-BR from all threats, whether internal, external, deliberate or accidental. Information within NIHR-BR exists in primarily electronic form and this policy intends to protect data stored electronically, transmitted across networks and less commonly on paper. The prime purpose of NIHR-BR's Information Governance policy is to protect and safeguard the information of the NIHR-BR and its participants.

1.3.2 The objective of information security is to prevent and reduce the impact of security incidents. The implementation of this policy is mandatory to maintain and demonstrate the organisation's integrity in dealings with all our external parties.

1.3.3 NIHR-BR information assets (e.g. data) are held primarily within an on-premise secure computing environment provided by an appropriately accredited 3rd party; thus NIHR-BR acknowledges that the primary computing environment may be subject to access and management by the above-mentioned 3rd party.A service level agreement (SLA) is signed by both parties with information security being a critical part of the agreement.

1.3.4 It is the policy of NIHR-BR to ensure:

- Information is protected against unauthorised access
- Confidentiality of information is assured
- Information is not disclosed to unauthorised persons through deliberate or careless actions

- The integrity of information is maintained
- Information is available to authorised users when required
- Regulatory and legislative requirements are met
- Business continuity plans are produced, maintained and regularly tested
- Information security training is delivered to all staff
- All breaches of information security, actual and suspected are recorded, reported and investigated

1.3.5 Standards, policies and security operating procedures are available to support this policy and include virus control, access control, personnel security and use of e-mail and the Internet. A formal disciplinary process operating through the employers of the individuals providing this service will be referenced and implemented for those employees who do not comply with standards, policies and procedures (see associated documents section above)

1.3.6 The IGRO, supported by the Information Governance Leads (IGLs), has overall responsibility for maintaining this policy and providing guidance on its implementation. All managers are responsible for implementing policies and procedures within their business areas. It is the responsibility of each employee to adhere to policies and procedures. Employees who do not adhere to the policies and procedures may be subject to disciplinary procedures.

1.3.7 This policy will be reviewed regularly to ensure it remains appropriate for NIHR-BR and in line with the regulatory framework.

2 Key Principles

The below-tabulated security principles have been selected to support staff in understanding their responsibilities for working securely with information and will help them in making security-conscious decisions in their day-to-day activities. These key Information Governance principles and their associated lower-level guidelines and procedures will ensure teams are working securely whilst maintaining standards in their ways of working with data.

Protecting Information	Our organisation is committed to maintaining the confidentiality, integrity and availability of information and associated systems. We remain committed to ensuring we always employ mechanisms for data protection, and governance when working with our data. All staff must equally appreciate their unique responsibilities for working to maintain the confidentiality, integrity, privacy, quality and availability of data by applying the principles in this policy and those outlined in the associated procedures and standards.
Data Protection and GDPR	Our organisation will maintain adherence to all applicable data protection legislation, including, where applicable the UK General Data Protection Regulation and Data Protection Act 2018. We will strive to ensure that we incorporate the below listed principles in our ways of working with data: 1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Data minimisation 4. Accuracy 5. Storage limitation 6. Integrity and confidentiality (security) 7. Accountability
Information Classification	Information will be classified in a manner that ensures its security and maintains its integrity. Information owners shall be responsible for assigning classifications to information assets according to the information classification standard.
Information Handling	All staff must adhere to the appropriate information handling procedures when on and offsite. Access to all information that is of value to the organisation and personal information will be restricted consistently with the information handling guidelines and procedures. All members of staff are expected to store any sensitive information in a secure location. Such informantion or physical assets must not be left unattended or in open view.

The organisation will ensure procedures and systems are in place to implement appropriate access controls, to ensure that information is stored and transported securely and is not lost or corrupted.

Our Physical data is of equal importance, and we aim to maintain a clear desk organisation, where data is only ever printed or maintained in a physical format where absolutely necessary and archived securely or destroyed by the approved destruction mechanisms upon termination of use.

Acceptable Use of Devices

Staff must ensure they read and understand the organisation's acceptable use policy. Staff are forbidden to access the organisation's personally identifiable data with a device that is not provisioned by the organisation and within the organisation's managed asset.

Staff must follow the organisation's incident reporting procedure to ensure any data related issues with their provisioned device.

User Access Management

The organisation will ensure that no individual is allocated responsibility for or given access to more parts of the system(s) than is necessary to perform their duties.

Where practicable, NIHR-BR's operations will be structured with roles and responsibilities allocated to avoid overlapping areas of interest between individual duties and roles. Where this is not possible supervision and shared controls will be used to minimise threats, which may arise from such overlaps.

Users – Terms and Conditions

Before gaining access to the NIHR-BR's secure systems, all visitors and external staff/partners must have agreed to a confidentiality and access agreement between their employer or agent and the University of Cambridge or Cambridge University Hospitals NHS Foundation Trust.

Users shall not at any time during access to the NIHR-BR's secure systems, or at any time afterwards, disclose to any person any information that would compromise the privacy of any individual participants, compromise the practical business dealings or affairs of NIHR-BR or as to any other matters which may come to their knowledge by reason of their access.

Users – Teleworking

Teleworking is defined as working at home or at any other private off-site locations that are linked electronically to a central office or principal place of employment. Teleworking is a cooperative arrangement between NIHR-BR and its employees, contractors, and associated personnel.

NIHR-BR is committed to develop, maintain and support a comprehensive policy of equal opportunities in employment within NIHR-BR. To assist in this NIHR-BR will actively support Teleworking where it is reasonable and practical to do so and where operational needs would not be adversely affected.

	Where staff are working offsite or teleworking, they are expected to adhere to the Teleworking policy (found in the Acceptable Use Policy) and ensure that they adhere to the published guidelines. (This policy does not apply to situations where a manager occasionally allows an employee to work at home on a temporary ad-hoc basis.)
Personally Identifiable Information (PID)	Other than to contact the participant themselves, Personal Identifiable Data (PID) can only be sent over secure communications channels that have been approved and tested by the NIHR-BR Information Security / Information Technology team, or are otherwise accredited by NHS Digital e.g. NHS Mail.
Defense in Depth	The NIHR-BR will seek to ensure that security mechanisms are layered in such a manner that the weaknesses of one mechanism are countered by the strengths of one or more other different mechanisms. This helps to provide resilience against different forms of attack and reduces the probability of a single point of failure or compromise.
Assign least privilege	Environments, systems and applications are configured to provide no more authorisation to any individual user account than is necessary to perform required functions. Consideration is given to implementing role-based access controls (RBAC) for various aspects of system use, not only administration.
Incident Management	The organisation will ensure a rapid response to incidents that threaten the confidentiality, integrity, and availability (CIA) of NIHR-BR's information assets and / or information systems, and require all staff to be understand their responsibilities for helping to prevent incidents or reduce their impact. Where security incidents arise through accidental, intentional misuse or negligence, a security incident entry shall be completed in the Incident Log once the incident has been identified. The competence of the individual(s) responsible shall be re-assessed. Training will be discussed if the incident is found to be accidental or unintentional and / or repeated.
Design for Updating	Security should be designed to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
Interoperability	Where possible, security of systems and applications will be based on open standards for portability and interoperability. For security capabilities to be effective, the team should make every effort to incorporate interoperability and portability into all security measures, including hardware and software, and implementation practices.
Separation of Duties	The Organisation will ensure the clear separation of tasks and functions between different roles to provide a layer of accountability and protection.
Secure Defaults	Every application, service and process should be implemented securely by default. Administrators should decide to reduce security only by exception

	and if the application and / or business process requires it, but default configuration settings should be the most secure possible.
Training and Awareness	NIHR-BR will implement a programme for providing appropriate information security awareness and training to all users / staff.
Privacy by Design	The organisation will always ensure that the introduction of any new systems or processes that involve personal data use is undertaken with the aim to protect personal information of individuals and ensure the application of privacy related regulations that are relevant to the organisational environment.
Security Culture	The organisation will ensure that all staff are adequately trained in and understand their role in achieving a sound security culture.
Zero Trust (Identity-Driven Access Control)	The NIHR-BR is adopting the principle of Zero Trust, which is based on the concept that network perimeters or boundaries are not as clearly defined any longer in governing access to data or other resources. Instead, trust (access) is granted to specific individuals in specific contexts for specific purposes. Trust isn't assumed, it is granted when the individual has demonstrated that they are who they say they are and have the appropriate authority.
Auditing and Monitoring	The NIHR BioResource will ensure that internal audits or spot checks are conducted on-site at the locations within the scope of compliance against the criteria for NHS IG Governance at least once a year.

3 Who Must Follow This Policy?

This policy is mandatory for all staff working within the NIHR BioResource. The NIHR BioResource is also committed to having its third-party partners and vendors meet the requirements set out herein. Depending on the seriousness, failure to comply with our policies may lead to disciplinary action.

Staff that choose not to follow the specified requirements contained within the security procedures and policies of the organisation shall be subject to the disciplinary process. The Disciplinary Process Procedure can be found in the Cambridge University Hospitals NHS Foundation Trust and University of Cambridge Human Resources documentation.

4 Questions and Support

For specific questions and or feedback on this policy, please contact:

- **The NIHR BioResource Information Governance & Information Security team**
  Email: ig@bioresource.nihr.ac.uk

- **The Data Protection Officer**

Michelle Ellerbeck
Information Governance lead/Data Protection Officer
Cambridge University Hospitals NHS Foundation Trust
Box 153
Hills Road
Cambridge
CB2 0QQ

Email gdpr.enquiries@addenbrookes.nhs.uk

5 Further Links

5.1.1 The NIHR BioResource organisation in acknowledging that it is not a legal entity, has sought and gained the oversight of the Information Governance team at Cambridge University Hospitals NHS Foundation Trust. Our Information Governance Policy is therefore to be followed in conjunction with the below associated policies to ensure a comprehensive understanding of all the obligations on the staff members of our organisation and consequently the University of Cambridge.

a. University of Cambridge, School of Clinical Medicine – Information Security Policy

https://www.medschl.cam.ac.uk/about/computing/information-security-policy/

b. Cambridge University Hospitals NHS Foundation Trust - Information governance and information security policy

https://www.cuh.nhs.uk/documents/58/Information_governance_and_information_security_policy_Version13_July_2017-2.pdf