INTEGRATED BIOBIOREPOSITORY OF H3AFRICA UGANDA

MAKERERE UNIVERSITY
COLLEGE OF HEALTH SCIENCES

POLICY

TITLE: **INFORMATION MANAGEMENT POLICY**	**PAGE 1 of 10**

POL #: **IBRH$_3$AU-POL-004.1**	Effective Date: **06/01/2014**	Next Rev: **DEC 2015**
Prepared by: (Signature & Date) NAME: Musinguzi Henry TITLE: Lab Manager	Reviewed by: (Signature & Date) NAME: Dr. Samuel Kyobe TITLE: Coordinator	Approved by: (Signature & Date) NAME: Prof. Moses Joloba TITLE: Principal Investigator

VALIDATION AND RETIREMENT

	NAME	DATE
Validated by:		
Retired by:		

ACKNOWLEDGEMENT OF READING AND UNDERSTANDING

I have received and understood the training on this Policy. If I have not understood the training I have asked the trainer to retrain me to ensure that I completely understand all the requirements.

	NAME	SIGNATURE	DATE
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Table of Contents

1 INTRODUCTION

Translational research, using advances in molecular biology, archived biospecimens and annotated data, is pursued to aid in the elucidation of the disease process and discovery of new diagnostic and treatment modalities. A collection of stored and well-annotated biospecimens and derivatives is a valuable resource, important to the research process. The quality of the biospecimen and the extent of the accompanying data is a determinant of value. The goal of the IBRH3AU is to standardize procedures for handling biospecimen and data thus ensuring that the quality and integrity of the collection is consistently maintained at a high level.

2 PURPOSE

The purpose of this Information handling policy is to give guidelines that will be followed when handling data and information generated during operations of the IBRH3AU

3 SCOPE

This policy applies to all IBRH3AU personnel involved in handling data and information

4 POLICIES

4.1 Audit Trail

The inventory system shall include a full audit trail of changes made to the database. This includes recording changes to both specimen data and system metadata. The audit trail shall include but not be limited to: the original data; the changed data; who made the changes; how the change was made, date and time of change, and if possible, why the changes were made. This audit trail shall be automatically recorded and available for read-only access. Record changes shall not obscure previously recorded information in the Audit Trail. Such audit trail documentation shall be retained for a period at least as long as that required for the electronic records and shall be available for agency review and copying.

4.2 Security

Access to the computerized inventory system shall be tightly controlled. Passwords shall conform to the minimum standards regarding password length, strength, life cycle, recycling, etc. Security roles with defined privilege levels shall be assigned to individual users of the system. Some individuals may be able to view specimen availability whereas others can enter or modify specimen descriptions and make requests to have specimens shipped from the biorepository. The system shall provide a mechanism to log off users after a specified period of time during which the system is idle. All database access attempts shall be logged with the date and time of login and logout. Any failures to access the database shall be logged with the date and time and reason

for failure. The system shall lock out a user after a specified number of failed attempts to access the system.

The inventory system shall provide for single system sign-on utilizing the operating system's user name and password if possible.

User authentication information shall always be encrypted.

All remote communication shall be able to be conducted on an encrypted socket (i.e., via a port that requires data encryption to prevent inappropriate access to secured data).

For example, Web based systems shall be able to implement data encryption using a Secure Socket Layer (SSL) at the browser level. All Protected Health Information (PHI) shall be secured within the database through access controls and/or encryption.

4.3 Interoperability

Within modern biorepository informatics systems, integration and interoperability are highly desirable. Systems shall be able to integrate with other local applications such as electronic medical records, cancer registries, pathology systems and freezer temperature monitors. This allows other systems to be the single source of truth (SSoT) for appropriate data.

Integration and interoperability have many benefits which include, but are not limited to, the following:

Reduced re-entry of data every time data is manually reentered from one system to another there is a risk of error. Re-entering of data can be costly.

Data errors found and corrected in the SSoT system shall be replicated to other systems.

Data shall be electronically convertible into formats that can easily be shared among collaborating institutions, where possible and appropriate. The inventory management system shall enforce all data integrity, security and audit trail requirements for external access. To achieve interoperability, inventory management systems shall do the following:

Have a public documented Application Programming Interface (API) to enable other systems to integrate with it. Use common public vocabularies for relevant data points.

4.4 Reporting

The inventory system must have the ability to produce reports to support the biorepository workflow, document adherence to standards and practices and provide any business metrics required by the biorepository.

The system shall provide the user with an interface for specifying display content and search criteria for the report. The exact nature of this interface can vary from full ‘‘what you see is what you get’’ (WYSIWYG) report designers to simple field selection for tabular reports. The query editor can also be presented utilizing several approaches, including simple data query forms, Query By Example (QBE) screens, customized query builders and text areas for native query specification.

The inventory system shall have the ability to save reports for future execution. The inventory system shall have the ability to generate report output and electronic data files (e.g., in ASCII, XML, or Excel format). The system shall provide full access to the database for reporting, provided that the system’s security rules are enforced. This access will allow users to generate reports on inventory status, freezer status, user access, audit trail entries, and other data tracked by the database to meet their needs.

If the database contains PHI records, the security model must restrict reporting on confidential data to only authorized users. Additionally, the biorepository shall maintain SOPs about the generation, use,and destruction of reports that contain PHI to ensure that donor confidentiality is maintained.

4.5 Validation

A closed system is defined as an environment in which system access is controlled by persons who are responsible for the content of electronic records that are in the system.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedure sand controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Protection of records to enable their accurate and ready retrieval throughout the records retention period

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction

Determination that persons who develop, maintain or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Use of appropriate controls over systems documentation including:

Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

4.6 Quality Assurance

In order to provide high-quality information to serve the tracking system, standards, policies, and procedures shall be used to ensure and maximize the quality, objectivity, utility and integrity of the data. Periodic reviews of data quality issues and adjustments to programs and processes will ensure continuous quality improvement. The electronic inventory system shall comply with industry-applicable guidelines. An established Quality Assurance program for the inventory system shall be primarily directed at prevention of non-conformances as well as detection, corrective action and process improvement implementation.

Regular Quality Assurance audits and reviews shall completely document:

User requirements, as well as industry-specific certification requirements

Details of the review and approval process for software developed in-house, or obtained from a third party.

Procedures followed to test the software functionality, compared with user requirements.

Corrective actions or processes used to handle program errors and modifications.

Training provided to personnel associated with the use (and development, if applicable) of the inventory system. A periodic audit of the database shall be performed to ensure accuracy of data.

4.7 Backup

Regularly scheduled backup procedures are an important security function that will enable the inventory system to be restored in the event original data is lost or corrupted, most typically due to drive or other hardware failures. The database shall be backed up on a regular basis, depending on the institutional policies and frequency of data modification. The more frequent the data is changed, the more frequently the backups shall be made.

The procedures to preserve the integrity of IT data shall include (but are not limited to) steps to limit the extent of the destructive event, protocols for periodic backing up and storing of information, procedures for off-site storage of backup data, and protocols/procedures for restoring information from backed up media.

The procedures shall specifically address the recoverability of information. Backups shall be validated on a regular basis to ensure the data can be accurately recovered.

Changes to hardware and software commonly require review and reevaluation of these documented procedures. These procedures must specifically address the physical environment and equipment.

4.8 Labels

Each specimen shall receive a label that tightly adheres under all projected storage conditions.

Information printed on labels shall be resistant to all common laboratory solvents. Labels shall contain an ID linking to a database containing details about the specimen collection and processing information Flexibility shall be allowed in the location of the label to allow for label legibility on a wide variety of containers.

Material used in composition of containers for some specimens may pose special problems for label adherence and therefore in some cases, the label shall be able to adhere to itself. The adherence of labels to containers as well as the use of particular types of ink shall be tested under conditions more extreme than the anticipated storage and processing conditions before they are put into regular use.

4.9 Labels for Specimens

Human specimens shall be labeled in such a way that protects privacy and confidentiality and is in compliance with applicable laws and institutional policies. Specimens shall be labeled with a unique code or ID not derived from information about the donor. No other study or personal health information shall be encoded in the specimen ID.

For all specimens, the biorepository's unique identifier for each specimen shall be printed on the label in both barcode format and human readable form. The ID shall not be reflective of its storage location in the biorepository, as locations may change over time.

4.10 Barcoding

Whenever possible, labels shall be printed with a barcode that uniquely identifies the specimen. Linear (1D) barcodes are adequate for small values and/or larger labels. Under some circumstances, two-dimensional (2D) barcodes are necessary. 2D barcodes have the advantage that scanning error rates may be lower, more information can be included on the label and they may be optimal for use on smaller vials. Some containers can be ordered preprinted, such as straws and small vials that fit in 96-position racks. In certain situations, preprinted containers can have an ID structure that alleviates applying another label onto the container and save supplies and labor. Each aliquot/container shall be labeled with a unique barcode/number.

4.11 Shipping log

The biorepository shall maintain a shipment log to record the receipt and dissemination of shipments sent to/from the biorepository. This log shall be integrated into the functionality of the inventory management system described above. Each shipment entry shall be given a unique shipment ID. The electronic log shall be able to track the following elements:

- Shipment/Invoice ID.
- Source.
- Destination.
- Date shipped and date received.
- Courier name.
- Package Tracking ID, if applicable.
- Unique sample identifier.
- Sample type(s).
- Quantity sent and received.
- Study name and/or number if available.
- Shipping conditions (e.g., dry ice, ambient, refrigerated, LN2)
- Name/Signature of individual receiving the shipment.
- Any discrepancies between the shipping manifest and the actual shipment.
- Any indication that a specimen has been compromised (e.g., record deviations in sample quality upon receipt).

5 REFERENCES

5.1 Best Practices for Repositories I. Collection, Storage and Retrieval of Human Biological Materials for Research, International Society for Biological and Environmental Repositories (ISBER) http://www.isber.org

6 REVISION HISTORY

Revision No	Effective Date	Description of Changes Made from Preceding Revision	Approved by/ Date

ANNEX 1: DOCUMENTATION OF SUGGESTED CHANGES TO THIS POLICY

CLAUSE	SUGGESTION	BY	DATE