SUNY Downstate Medical Center -University Hospital of Brooklyn Network
Department of Pathology Policy and Procedure

Subject: DATA SECURITY POLICY - DEPARTMENT OF PATHOLOGY

Prepared By: Maria Yudlowitz

LTR: LTR14015

Edit Approved By: Howanitz MD, Peter (Electronic Signature Timestamp: 1/13/2014 10:00:08 AM)
Laguerre MS, Alix (Electronic Signature Timestamp: 1/9/2014 10:54:24 AM)
Yudlowitz, Maria (Electronic Signature Timestamp: 1/7/2014 4:44:00 PM)

Reviewed By: Zuretti MD, Alejandro (11/13/2014 1:59:53 PM)

Supporting Documents: Lab-26

Approval Workgroup: LIS Policy Approval

Revision: 2.5

Purpose:

The purpose of this policy is to ensure that patient information is protected from unauthorized disclosure and is safeguarded to prevent unauthorized modification or destruction.

Scope:

The Clinical and Anatomic Pathology Laboratories in the Department of Pathology are committed to security and confidentiality of patient data.
Security and confidentiality of patient information is a matter of concern for all persons who have access to patient information.
Each person accessing data holds position of trust relative to the information and must recognize the responsibilities entrusted in preserving the security and confidentiality of its contents.
All laboratory personnel who are authorized to access data must read and comply with this policy.

Objective:

- To provide security standards for management, storage, and distribution of patient information.
- To promote consistent protection and security of patient medical records.
- To communicate the responsibilities for the protection of data and foster information security awareness to the laboratory staff.
- To facilitate appropriate access to patient information by those who have a specific authorized patient-care or business needs or other legally authorized need for access.
- To assist laboratory personnel utilizing patient data in complying with requirements for confidentiality and privacy established by state laws, CAP, JCAHO, The Joint Commission and Accreditation of Healthcare Organization, HIPAA, and other regulatory agencies.

VENDOR/CONTRACTORS/RESEARCHERS:
All vendors, contractors, and researchers are required to sign a confidentiality statement prior to any information system or data access.
(See attachment I)

BREACH OF DATA SECURITY POLICY:
Any violation of the Laboratory Data Security Policy, which might include acts such as negligence in releasing patient information or breach of patient confidentiality, could result in severe disciplinary actions. These penalties could include formal reprimand suspension or loss of employment.
(See Attachment II)

USER AUTHENTIFICATION AND ACCESS CONTROL:
The Laboratory Information System provides for user authentication, access control, accountability strategies and security reports.
(See Security Policy – Laboratory Information Systems)

ATTACHMENT I

(Data Security Policy)

VENDOR DATA SECURITY AND CONFIDENTIALITY AGREEMENT FOR ACCESS TO LABORATORY DATA, INSTRUMENT, AND INFORMATION SYSTEM

POLICY:
The Department of Pathology will permit Prospective Vendors to have access to Laboratory Data, Instruments, and Information Systems, subject to the following conditions:

- Vendor will only access information necessary to provide technical support systems or applications associated with their company for troubleshooting.
- Vendor acknowledges that all information accessed is the property of University Hospital of Brooklyn and is therefore confidential.
- Information obtained will not be copied, released, altered, or destroyed without proper authorization from the Department of Pathology.
- Vendor will safeguard and will not disclose access code or any information that allows access to confidential information.
- Vendor will accept responsibility for activities undertaking using assigned access code or other authorization.
- Vendor understands that failure to comply with this Policy may result in immediate termination of access and possible legal action against the company.

Signature of Vendor Staff Member: _____ **Date:** _____

Name and Address of Vendor: _____

_____

_____

Department Contact Signature: _____ **Date:** _____

ATTACHMENT II
(Data Security Policy)

Data Security Awareness

Objective:
All laboratory employees will be trained through our continuing education programs regarding the need for data security awareness, to improve security practices, and to protect individual confidentiality. Each employee's Performance Evaluation shall assess the employee's compliance to the confidentiality policies.

The following data security policies are applicable to all laboratory personnel regardless of their classification.

- Observe the privacy and rules governing the use of any patient information accessible through computer systems or ledgers and only access information necessary for performance or your duties.
- Follow the procedures established to manage the use of each information system.
- Prevent unauthorized use of any information in files maintained, stored, or processed by information systems.
- The system administrator will give individual passwords to each employee. Password given to each employee to access data must be kept confidential and should not be disclosed to any other employee or employees.
- Sign immediately from any system after accessing required data.
- Do not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through assignment.
- Disclosing the contents of any record or report except to fulfill a work assignment is prohibited.
- Do not knowingly include or cause to be included in any record or report, a false inaccurate or misleading entry.
- Understand that the information accessed through all information system contains sensitive and confidential patient care, business, financial, and hospital information, which should only be disclosed to those authorized to receive it.
- Disclosing patient information for unauthorized purposes is prohibited.
- Report any violation associated with data security.
- Patients, family members or friends seeking laboratory results should request information from the Health Information Management Department or **other Healthcare provider**.
- The hospital policies for telephone and facsimile requests must be followed.(see UHB policies AD-2 & AD-3)

ATTACHMENT III
(Data Security Policy)

EMPLOYEE ACKNOWLEDGEMENT OF RECEIPT
OF THE
UHB LABORATORY DATA SECURITY POLICY

- I acknowledge the receipt of the UHB Laboratory Security Policy.
- I understand that this policy serves as a laboratory employee guide for Data Security and confidentiality.
- I understand that it is my responsibility as an employee of UHB to review and use all applicable information contained in this policy in performing my duties.

Signature of Employee: _____ **Date:** _____

Signature of Supervisor: _____ **Date:** _____