Pathology

SUNY DOWNSTATE MEDICAL CENTER
UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

Subject: UHB/CERNER LABORATORY INFORMATION SYSTEM (LIS) SECURITY	**No:** LAB- 22
	Page: 1 of 4
	Original Issue Date: 11/07
	Supersedes: 01/09
Prepared by: Dorothy Kirk 3/9/10 Maria Yudlowitz	**Review Date:** 02/10
Reviewed by: Maria I. Mendez 3/8/10 Alix R. Laguerre 3/5/10	**The CAP Standards:**
Approved by: Peter J. Howanitz, MD	**Issued by:** Pathology

Introduction:

UHB/Cerner Laboratory Information System is designed to protect all laboratory information that is ordered, collected, processed, and stored on all patients registered into the system.

Security methods for safeguarding against the inappropriate access to information, unauthorized changes to information, and lack of availability of information is maintained through a variety of system and application software.

Policy:

1. All employees must be authorized to use the system.
2. All users must be trained before they are authorized to use the system.
3. Each user will be assigned various applications based on their hospital title.
4. Users will be given their unique username and password after training.
5. Each user must use their username and password to log into their assigned applications.
6. No user shall use another employee's username and password to log into the system.
7. Each user must log-out immediately after using an application. If a user does not log-out of an application, he or she will be held accountable for any changes, modifications, or inquiries that may occur in that application via their log-on for that period.
8. Each user is allowed to change his or her password at will if the old password is known.
9. System Security Administrators are allowed to reset user's password without knowing the old password.
10. When an employee no longer uses the system his or her username and password will be inactivated.

11. Any user who gives access to another user via their username and password will be removed from the system.

12. All users must conform to the hospital patient confidentiality statement written on the desktop of each computer.

13. All users must conform to the warning sign written on the screen saver of each computer which states:
"THIS IS A MEDICAL INFORMATION SYSTEM DEVICE, ANY ADDITION OF SOFTWARE OR MODIFICATION OF THE CONFIGURATION WILL RESULT IN SEVERE DISCIPLINARY ACTION."

14. Database Administrators are authorized to:
    - Order laboratory tests
    - Enter or access patient data
    - Enter results
    - Change results
    - Change billing
    - Modify programs and applications.
    - Upgrade software
    - Modify software

15. System Administrators are authorized to:
    - Upgrade software
    - Modify software
    - Upgrade hardware
    - Modify hardware

16. Laboratory Supervisors, Assistant Supervisors, and Laboratory Administrators are authorized to:
    - Order laboratory tests
    - Enter or access patient data
    - Log-in specimens
    - Enter results
    - Change results

17. Laboratory Technologists and Technicians and Phlebotomists are authorized to:
    - Order laboratory tests
    - Enter or access patient data
    - Log-in specimens
    - Enter results
    - Change results.

18. Laboratory Clerks are authorized to:
    - Order laboratory tests
    - Enter or access patient data
    - Log-in specimens

19. Nurses, Suites and Nursing Station Clerks are authorized to:
    - Order laboratory tests
    - Enter or access patient data

20. Physicians, HIV Counselors Nurse Practioners and Head Nurses, are authorized to:
    - Order laboratory tests.
    - Enter or access patient data.
    - Access HIV results.

21. Med Tech Students are authorized to:
    - Enter of Access patient data

22. Physician Viewer
    - Enter or access patient data.
    - Access HIV results.

22. Point of Care personnel
    - Order laboratory tests
    - Enter or access patient data
    - Log-in specimens
    - Enter results for Point of Care tests

Procedure:

The Cerner's HNA Millennium architecture provides four areas of security:

a) User authentication
b) Access control
c) Accountability strategies
d) Security reports.

User Authentication:
User authentication is the process of positively identifying a user through the use of usernames and password. Its purpose is to authenticate, or confirm, the identity of the user. It is required by every application within the UHB/Cerner information system.

Three pieces of information are required at the time of log-on: user name, password, and domain. The system locates the security server in the **domain** specified and determines whether the **user name** and **password** are valid. The system accomplished this task by using an encryption algorithm.

The HNAUser Tool application is used to create and maintain user names and passwords.
Access Control:
Access control is the process by which an authenticated user is given access to various groups of applications by their positions assigned. The positions are created and assigned by the database administrators.
The positions assigned are:

a) Database Administrator
b) Administrator
c) Lab. Supervisor
c) Lab. Technologist
d) Lab. Clerk
e) Phlebotomy
f) Physician
g) Nurse Administrator
h) Head Nurse
i) Nurse
j) HIV Counselor
k) Clerk
l) Non-Lab (unspecified)
m) Med Tech Student
n) Physician Viewer
o) POC

A user is assigned a position through the User Maintenance Tool.
Positions are created as code values in the CRMCode Tool.

Associated with each position is the applications to which each user is allowed access.
These applications are organized into “application groups”, which are directly related with one or more positions. Application groups are created in the Task Access Tool.

Accountability Strategies:
Accountability strategies are audits setup in the system to monitor and record all users activity when logged into the system. This is designed to encourage all users to make appropriate use of the information they are authorized to access within the system.

Security Reports:
Various security reports are readily available.

Security Features:
The following is a list of security features that are available in the system.

1) System provides for the use of both user name and password to verify authorization.
2) System provides the use of alphanumeric username.
3) Usernames are unique and specific to one user.
4) Passwords are unique and specific to one user.
5) System permits the security administrator to reset passwords without knowing the old password to unique value.
6) System forces user to select a password at initial sign-on and when the password has been reset.
7) System permits users to select their own password without assistance or involvement of a security administrator.
8) System allows users to change their password at will.
9) System permits the security administrator to specify a password expiration interval.
10) System permits specifying a password interval on a per user or per class of user basis.
11) System automatically prompts users to enter a new password upon password expiration.
12) System provides message to user upon denial of access due to an invalid user name or password.
13) System supports automatic disabling of a user name or password after consecutive invalid access attempts.
14) System supports a hierarchy of security administration.
15) System is designed to permit highest level security administrators to delegate specific access to department security administrators.
16) System permits security administrator to disable a user name without deleting it from the system.
17) System supports the real time disabling of a user name or password.
18) System supports the security administrator’s ability to define and control vendor access.
19) System allows single sign on across domains.
20) System provides reporting and maintenance tools for the security administrator.
21) System allows user to restrict printing and display of confidential data elements (e.g., HIV).
22) System provides control over stored data to ensure data is complete and consistent.
23) System provides the ability to store all rejected transactions along with a reason for the rejection.

System is protected from unauthorized access via internet through the use of firewall, and authentication devices.