Pathology

SUNY DOWNSTATE MEDICAL CENTER
UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

	No: LAB- 27
Subject: UHB/COPATH ANATOMICAL AND PATHOLOGY INFORMATION SYSTEM SECURITY	**Page:** 1 **of** 3
	Original Issue Date: 1/02
	Supersedes: 11/07
Prepared by: Alix R. Laguerre, MS	**Review Date:** 1/09
Reviewed by: Maria I. Mendez, MA	**The CAP Standards:**
Approved by: Peter J. Howanitz, MD	**Issued by:** Pathology

Policy:

CoPathPlus Anatomical Pathology 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 are maintained through a variety of system and application software

Procedure:

The CoPathPlus 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 CoPathPlus 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** is valid. The system accomplished this task by using an encryption algorithm.

The Permission and the Person Dictionaries are 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. These positions are created and assigned by the database administrators.

The permission groups assigned are:

(a) Database Administrator
(b) Pathologist
(c) Clinician
(d) Transcriptionist
(e) Cytology Supervisor
(f) Cytotech
(g) Histotech
(h) Inquiry

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 passwords 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 invalid user name or password.
13. System supports automated 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 the highest level of 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 allows 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 provides control over stored data to ensure data is complete and consistent.
22. 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.