Department of Health, Bureau of Public Health Laboratories
Computer Use and Confidentiality Agreement

The Florida Department of Health (DOH) has provided you with the Computer Use and Confidentiality Agreement and Policy & Procedures. This document governs all users of DOH computer systems.

Understanding of Computer Related Crimes act:

The Department of Health has authorized you to have access to confidential data as defined by Chapter 382 Florida Statutes, through the use of the DOH WebLIMS Portal to access patients' sample reports in LabWare.

Computer crimes are a violation of the department's policy and Florida Statutes. The commission of computer crimes may result in disciplinary action by their facility and criminal procedure by the department. The Florida Computer Crimes Act, Chapter 815, Florida Statutes, addresses the unauthorized creation, modification, destruction, or disclosure information resources.

In addition, Ch. 382.026, F.S., specifically states that any person who, without lawful authority and with the intent to deceive, makes, counterfeits, alters, amends, or mutilates any certificate, record, or report commits a felony of the third degree.

I have read the above statements, and by my signature, acknowledge I understand that a security violation may result in criminal prosecution according to the aforementioned provisions of Chapters 815 and/or 382, Florida Statutes.

The minimum information security requirements are:

- Information entered in the LabWare system and accessed through the WebLIMS portal is confidential by law and shall not be disclosed to unauthorized persons.
- Personal passwords are not to be shared nor disclosed. There may be supplemental operating procedures that permit shared access to electronic mail for the purpose of ensuring day-to-day operations of the department.
- No supervisor may order a user to share his or her password.
- All user-level passwords must be changed at least every 90 days.
- Information, both paper-based and electronic-based, is not to be obtained for my own or another person's personal use.
- Department of Health data systems must be used for official state business.
- No user of a DOH system may create fraudulent records.
- Copyright law prohibits the unauthorized use or duplication of software.
- When computers are left unattended, users must lock their computers.

_____	_____
Signature of User	Date
_____	_____
Print Name of User	User's Facility Name

Please fax or email Page 1 only to:
(904)-791-1567 or DLBPHLLAR@flhealth.gov

Policies and Procedures

This Computer Use and Confidentiality Agreement will be completed by each user prior to receiving access to the e-Vitals system. This system allows the user to access confidential information and information technology resources.

- All users with access to confidential information must sign the Computer Use and Confidentiality Agreement (CUCA).
- The signed CUCA form will be maintained by the Bureau of Public Health Labs.
- The respective Florida Statutes may be found on the website: http://www.leg.state.fl.us/Statutes
- The Florida Computer Crimes Act, Ch. 815, F.S., prohibits the introduction of fraudulent records into a computer system, the unauthorized use of computer systems and facilities, the alteration or destruction of computerized information, and the stealing of data from computer files. Computer crimes violate the department's policies and may result in criminal charges. Any users found to have violated these policies, laws, regulations, etc., may be subject to disciplinary action by their facility and criminal procedure by the department.
- Supervisors may monitor computer use by direct observation, review of computer history files through the systems administrator, or review work productivity and quality.
- Users will be given a user account to access DOH information technology resources. Users who are responsible for a user account within the department's network are responsible for taking the appropriate steps to select and secure their passwords.
- **Passwords** are an important aspect of information security. Authorized users are responsible for the security of their passwords and user accounts. ○ Personal passwords may not be shared or disclosed. ○ No supervisor may order a user to share his or her password.

  ○ All user-level passwords must be changed at least every 90 days.
- When computers are left unattended, users must lock their computers.
- Creating security breaches or otherwise disrupting network communication is unacceptable. Security breaches include, but are not limited to, unauthorized access of data not intended for the user, or logging into a server or account that the user is not expressly authorized to access.

Please fax or email Page 1 only to:

(904)-791-1567 or DLBPHLLAR@flhealth.gov