ATTACHMENT A

LOUISIANA STATE UNIVERSITY HEALTH SCIENCES CENTER
at New Orleans

HIPAA TRAINING EMPLOYEE CONFIDENTIALITY AGREEMENT

Please read the information below and sign at the bottom.

PATIENT RIGHTS

Individuals receiving healthcare services through LSU System facility have entrusted the staff and have been given the assurance that all information is held in strict confidence in accordance with legal requirements. Any information about a patient's condition, care, or treatment must not be discussed with anyone, either at or away from the LSU System facility, except with those who are in "need to know" situations.

Carelessness or thoughtlessness leading to the release of this information is not only unethical and possibly illegal, but will be referred to the Privacy Officer for investigation, and possibly the Human Resources Department for disciplinary proceedings.

Any breach of a member's right to confidentiality of legally protected health information by an employee of the LSU System Facility, that employee is subject to the disciplinary action of that LSU System Facility, up to and including possible immediate termination. For purposes of this policy, the word "employee" includes not just employees of the LSU System facility, but the entire workforce as defined by the HIPAA Privacy Rules.

PATIENT PROTECTED HEALTH INFORMATION (PHI)

The following items are patients' protected health information (PHI) as guaranteed by the Health Insurance Portability and Accountability Act of 1996:

- Names
- Addresses
- Dates, such as birth dates, or dates of service
- Telephone, fax numbers, and email addresses
- *Any* number that can be used to track a member
- Medical device numbers used by the member
- Pictures of the member

- Any other information that can be used to identify the patient

All **computer system PHI** information must be secured by:

- Setting screen saver passwords. The duration time should be set to five minutes.

All **printed documents with PHI** must be secured by:

- Printing out only that PHI which is absolutely necessary to perform your job.
- Minimizing work in progress documents that contain PHI on your desk or in your immediate work area.
- Putting away all documents with PHI at the end of the day. These documents need to be secured inside a closed drawer or file cabinet. A locking cabinet is preferred if available.
- Shredding all documents with PHI that are not needed in the designated, secure company shred box. If material with PHI is received offsite, it must be shredded offsite or returned to LSUHSC for shredding. All documents with PHI need to be put into the company shred boxes by the close of each business day.
- Enclosing all printed documents with PHI sent to other departments in an Inter-Department Delivery envelope, properly identifying the receiving and sending parties on the envelope.
- Carrying all documents with PHI that leave the office in a secure briefcase, folder, or audit bag.

COMPUTER PASSWORDS and ACCESS

- All passwords must be kept confidential.
- All passwords must be eight characters or more.
- Please use passwords that are not in a dictionary and that are not proper names (i.e., Charlie, Chicago, etc.). Should someone try to get into our network, passwords like these can be "guessed" by very simple programs.
- When selecting a new password, try using a password that is comprised of the first letters of a phrase that is meaningful to you. It is recommended that letters and numbers be mixed in your passwords.
- Do not share your passwords with other users. These passwords should be treated the same way you would treat your PIN number for your ATM card.
- If you have given out your password, or suspect that someone might know it, please contact the Information Security Administrator.
- Passwords should not be left on a sticky note attached to your monitor or anyplace else on your desk. If you must write it down, please put it in a secure location.
- When using computer dial-in access, protect PHI from those who could be looking at your computer screen.
- Computer access is limited by your actual job duties. Should your duties change, your access may be changed accordingly.
- Computer access is terminated immediately upon employee resignation or termination.
- Remember, if someone is signed on with your account and password, you, not the person who is masquerading as you, are responsible for all that is done.

EMAILS and FAXES

All LSU System facility correspondence transmitted by email and/or FAX must contain the appropriate confidentiality statement.

OTHER CONFIDENTIAL BUSINESS PROPRIETARY INFORMATION

The LSU System facility maintains a policy that all business proprietary information, including but not limited to strategic plans, marketing plans, financial prospects and results of operations, and other similar information that we use to operate in the marketplace, is confidential and may not be shared or discussed with anyone other than those employees or business associates who have a "need to know" and/or with whom we have a LSU System facility-approved business reason. Violation of this policy can also lead to disciplinary action, up to and including immediate termination.

EMPLOYEE ACKNOWLEDGMENT

I have read the above policy on members' rights and PHI, computer passwords and access, and confidentiality and agree to comply with it. I acknowledge that any violation of this policy by me may lead to immediate disciplinary action, up to and including the termination of my employment. I also acknowledge that my obligation of confidentiality continues to exist even when I leave the employ of the LSU System facility.

_____
Employee Name (printed)

_____ _____
Employee Signature Date

_____ _____
Human Resource Manager's Signature Date