DEVICE AND MEDIA CONTROL POLICY

PURPOSE

The purpose of the Device and Media Control Policy is to establish a companywide system to inventory, store, transfer, reuse and dispose of electronic equipment and storage media used in conjunction with Protected Health Information (PHI).

SCOPE

This policy applies to all LADD employees and Business Associates.

POLICY

It is the policy of LADD to establish procedures that adequately protect, maintain and destroy electronic equipment and storage media in a timely manner and provide a mechanism for reporting and resolving violations of this policy.

STANDARDS AND DEFINITIONS

The IT Director – Is responsible for insuring IT assets are documented and identifiable throughout the entire IT asset lifecycle, which includes:

- A full and complete inventory of all IT assets
- A record of PHI removal prior to IT asset re-use at LADD
- A record of movement, transfer or temporary sign out of all IT assets
- The ability to retrieve an exact copy of the PHI prior to movement or destruction of all IT assets
- A record of the destruction of all IT assets

- Ensure all IT assets are maintained and renewed according to the defined asset specifications and expected life.
- Utilize the current Technology Plan to guide IT asset purchases.
- Leverage existing licensing and purchasing agreements to ensure maximum buying power and value from purchases.
- Maintain a list of standard supported IT assets which are recommended for use at LADD.
- Ensure effective functioning for the planned lifecycle of the asset including planning for the eventual replacement of the asset.

IT assets are:

- Fixed computer equipment, e.g. servers, desktop computers;
- Portable computer equipment, e.g. laptops, mobile phones, tablets; MiFi's
- Processing peripherals, e.g. printers, photocopiers; fax machines
- Storage Media, e.g. hard drives, USB storage devices, network attached storage;
- Software, e.g. desktop business applications, operating system, administration software;
- Databases and data stores;
- Audio Visual equipment, e.g. projectors, smart boards, controls systems;
- Network infrastructure, e.g. routers, cabling, telecommunications;

Technology Disaster Recovery Plan – This plan is part of the Annual Strategic planning process and outlines the action taken to secure, recover, store and dispose of all company IT assets. The plan works in conjunction with this policy and the Record Retention and Asset Management Policy to ensure appropriate use and disposal.

Asset Custodian – The LADD employee responsible for implementing appropriate protection and maintenance of IT assets. Asset Custodians will maintain assets, including any preventive or scheduled regular maintenance and for completing periodic audits to ensure the ongoing accuracy of the asset register/inventory.

Asset User – The LADD employee assigned an IT Asset to perform their assigned job. Asset Users must protect and use the asset as intended. In the event of theft, loss or damage to the asset the individual, must immediately report the incident to the IT Dept. or their supervisor. Asset Users sign for and acknowledge their responsibility to immediately report theft, loss or damage to their assigned asset.

IT Assets must be returned to the IT Dept. at the termination of employment.

PROCEDURE

Following the general outline provided by the current year Technology Plan the following procedures will be followed by all employees:

1. Purchases of IT assets must go through the IT Department.
2. Prior to employees submitting IT equipment request to the IT Dept., approval must be sought by the employee's Director.
3. The Director will submit requests to the IT Director.
4. The IT Director will submit request to either the Director of Quality Improvement or the Director of Business depending on the cost and nature of the asset. Approval by the Steering Committee may also be necessary.
5. Once approved the asset will be ordered by the IT Director.
6. Once the asset has arrived at the LADD office the Asset Custodian will use the asset tagging system to create an accounting of the asset that includes:
   - Labeling the asset as property of LADD
   - Include serial or identification numbers
   - Assigning the user of the asset, if a single user is not able to be named the location assigned to the asset will be noted
   - The type of asset
   - The date the asset was purchased
   - The location of the asset (if not already noted above)
   - The value of the asset (if appropriate).
   - The accounting must be updated when an asset is approved for re-use or disposal
7. The IT Director will insure all USB ports are disabled in a way that prevents the use of thumb/zip drives or other removable storage devices.
8. The IT Director will coordinate the pick up or delivery of the asset along with all required training for the use of the asset. A record of the training must be collected and maintained in the IT Dept.
9. Periodic maintenance must be completed according to the manufacturer.
10. When IT assets are transferred to another location, a copy of the information available on the asset will by obtained by the IT Dept. prior to the transfer. After verifying a successful copy has been made the asset will be wiped clean according the disposal method specified below. The copied information must then be made available at the original location to maintain the continuity of information. A record of such movements must be maintained by the IT Dept.
11. At the end of the asset's lifecycle, the IT Dept. will collect the asset and complete any of the following disposal methods deemed necessary.

DISPOSAL

Computer equipment often contains parts, which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and

other storage media contain various kinds of EPHI. In order to protect EPHI all storage mediums must be properly erased and irretrievably destroyed in accordance with the Record Retention and Asset Management Policy.

Computer equipment for purposes of disposal refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes.

All computer equipment will undergo secure erasure of all storage mediums in accordance with current industry best practices. All data including, all files and licensed software shall be removed from assets using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense Standards through the Company Called SIMS.

No computer equipment will be disposed of in dumpsters, landfill etc. Under certain conditions the IT Dept. may arrange for electronic recycling bins to be placed at different locations where LADD provides support.

All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

The IT Dept. will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the department staff who performed the disk wipe.

Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Prior to leaving LADD premises, all equipment must be removed from the Information Technology inventory system.

No computer or technology equipment may be sold to any individual unless approved in advance by the Steering Committee.

MEDIA REUSE

Any equipment or storage media that contains confidential, critical, internal use only, and/or private information will be erased by appropriate means or destroyed before the equipment is reused.

DATA BACK UP

Retrieval of all EPHI and other LADD data is backed up and tested on a regular basis according to the Disaster Recovery Plan.

VIOLATIONS

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including separation from employment.