



HIPAA SECURITY AND SAFEGUARD POLICY

PURPOSE

To establish standards for the use of protected health information in accordance with federal, state and contract requirements.

SCOPE

This policy applies to all LADD employees at all locations.

POLICY

It is the policy of LADD to protect the privacy and confidentiality of protected health information for the people we support and the employees of LADD. The following safeguards/security measures have been implemented to ensure this privacy protection.

STANDARDS AND DEFINITIONS

1. All LADD Communication, Documentation, Storage Systems and Data Systems are considered to be part of the HIPAA Security and Safeguard Policy which include but are not limited to these medium/modes:
 - a. Telephone
 - b. Cell phones whether it be a LADD device or a personal device,
 - c. Email
 - d. Text
 - e. Recording devices
 - f. Voice mail
 - g. Faxes
 - h. LADD databases
 - i. EHR- Electronic Health Records
 - j. Computers/laptops/tablets whether it be a LADD device or a personal device that are used to access, the internet, web based data systems and LADD work products
 - k. Protected Health Information in paper and electronic formats,
 - l. Confidential employee information in paper and electronic formats
 - m. Any function related to employment with LADD and result in the production or receipt of information, documentation or messages created, sent, received, accessed, or stored collectively constitute company records and property and therefore the following expectations must be followed by all employees at all times;
 - i. Email and any usage of LADD computers and/or tablets are not to be used in any way to harass, defame or humiliate. Electronic communications may not contain content that a reasonable person would consider to be defamatory, offensive, harassing, disruptive, or derogatory, including but not limited to sexual comments or images, racial or ethnic slurs, or other comments or images that would offend someone on the basis of race, gender, national origin, political beliefs, disability, sexual orientation, gender identity, pornography, religious or political beliefs, national origin or disability. Employees who receive any emails via company computers or from other employees with this content must report the matter to Corporate Compliance immediately.
 - ii. The LADD electronic communications systems are to be used to conduct company business. Employees may not use the electronic communications systems for political causes; football pools or other sorts of gambling; illegal activities; seeking/inquiring about job opportunities outside of the organizations; non-work purposes; solicitations or advertisements for unrelated work purposes; social media; dating websites; or creating, possessing, uploading, downloading, accessing, transmitting, or distributing materials of a sexual nature. Employee communications need to align with the organization's MVV.

- iii. Employees may not use LADD's electronic communications systems to post non work-related information, opinions, or comments to Internet discussion groups, Social Networking sites and other such forums. Employees are prohibited from passing off their views as representing those of LADD.
 - iv. Computers and/or tablets cannot be used for the transmission or viewing of profanity, adult related material, sexually explicit or otherwise offensive material.
 - v. Electronic communications must be positive, motivating and fit the Mission, Vision and Values of LADD.
- n. There should be no expectation of privacy in anything accessed, created, stored, sent or received on the company's computer and data systems. Any computer activity during work hours or on LADD computers, systems or network, including messages, may be viewed by LADD without prior notice and should be considered the property of LADD.
 - o. Virus protection is maintained by the IT Department. No other forms of virus protection software are to be used or downloaded.
 - p. All transmissions of confidential information must be encrypted as specified by the HIPAA Security Rule.
 - q. Employees must maintain a log-on password for all applications accessed on the computer. Passwords must contain a combination of upper and lower case letters, numbers and functions. Ex: 1L#dd\$
 - r. Social Networking sites are subject to the HIPAA confidentiality standards regardless of time of use.
 - s. Employees cannot download or add any programs to company computers without IT Department approval. Removable storage devices are not to be used.
 - t. Any portable device such as a laptop, tablet, cell phones with data access abilities, etc. will be password protected to insure no violations of confidentiality occur. Passwords must contain a combination of upper and lower case letters, numbers and functions. Ex: 1L#dd\$ Employees are never to give out their passwords or log in information.
2. Employees may not upload, download, or otherwise transmit copyrighted, trademarked, or patented material, trade secrets; or other confidential, private, or proprietary information or materials in violation of any legal constraints. Employees may not upload, download or otherwise transmit any illegal information or materials. Employees may not use LADD's electronic communications systems to gain unauthorized access to remote computers or other systems or to damage, alter, or disrupt such computers or systems in any way, nor may employees, without authorization, use someone else's code or password or disclose someone else's code or password, including their own. Employees may not enable unauthorized third parties to have access to or use LADD Electronic communications systems, nor may employees otherwise jeopardize the security of LADD's electronic communications systems.
3. Employees must use the utmost care in creating electronic communications. Even when a message has been deleted, it still exists on a back-up system, can be recreated, printed out, or may have been forwarded to someone else without its creator's knowledge. As with paper records proper care should be taken in creating electronic records, which may someday have to be produced in connection with legal and/or business needs. Paper documents created and received by an employee, it is each employee's responsibility to ensure that those electronic messages that should be retained are in fact saved. Those messages that need not be retained should be deleted.
4. Any files downloaded from the Internet and any computer disks received from non-LADD sources must be scanned with virus detection software before installation and execution. The intentional introduction of viruses, attempts to breach system security, or other malicious tampering with any of your employer's electronic systems including the LADD databases and website are expressly prohibited and employees may face criminal prosecution.
5. All information accessed by employees either in electronic or written format will be done on a need to know basis. Unauthorized access to information not needed to complete job responsibilities is prohibited.

6. LADD employees may be using electronic systems/databases in conjunction with contract agencies; and therefore, will be required to follow additional security standards (such as no printing of materials) set by those agencies in addition to all of the above rules.
7. LADD reserves the right to monitor, access, retrieve, read, and disclose to law enforcement officials, contract agencies or other third parties all messages created, sent, received, or stored on the electronic communications systems without prior notice to the originators and recipients of such messages. Authorized employees may monitor the electronic communications of employees to determine whether there have been any violations of law, breaches of confidentiality or security, communications harmful to the business interests of LADD, or any violations of this policy and any other company policy and communication sent via LADD computers or cell phones is the property of the corporation. Data created by Authorized Users that is on the LADD Information Technology Network is the property of the LADD. There should be no expectation of privacy in anything created, stored, sent or received on the company's computer system.

PROCEDURE

Employees of LADD are required to do the following:

1. To protect the privacy of the people's individual records:
 - a. Sign-out individual records when removing from the home, including the following information:
 1. Name of record leaving the home
 2. Date
 3. Employee Signature
 4. Destination
 5. Employee must sign again when record is returned and in place in the program.
 - b. While out of the program, employees must secure the record(s) at all times. This includes whether the record is on their person or locked in the vehicle as required. Employees must ensure that no information is visible at any time including through windows. This policy will be strictly enforced.
 - c. Employees must take steps to ensure people who do not have a need to know or have permission to see information regarding the individuals we support do not have access to any individual records, information, etc.
 - d. When employees leave the program, they are responsible for securing the premises by locking all doors.
 - e. Records are to be secured in the programs at all times. Records must be secure in a manner that they are not readily recognized or available. Unauthorized persons cannot not have access; therefore, records are not to be left unattended.
2. Carrying confidential records:
 - a. Lock records in trunk, when possible.
 - b. If records have to be left in vehicle for a short amount of time ensure vehicle is locked and records are out of sight.
 - c. Records must not be left in vehicle for an extended period of time, i.e. overnight.
3. Any devices, whether it be a LADD device or a personal device, containing confidential material (i.e. laptops, cell phones with data access abilities, tablets, day-runners, planners, etc.) must be kept secure at all times and must be password protected. **The storage of confidential material on removable storage devices is prohibited.** All devices must be set to contain the approved LADD confidentiality statement at the bottom of any business related communications.
4. Verification of Identification:
 - a. Employees must ask for identification to verify the authority of anyone requesting entry into the program.
 - b. Employees must ask for identification to verify the authority of anyone requesting information regarding the person or program.
 - c. Employees must make reasonable attempts during phone conversations to verify the caller. Attempts could include obtaining the person's contact information, hanging up the phone and verifying the

accuracy and authority or providing the contact information to a member of management so they may contact the individual.

5. Faxing: Employees should make reasonable attempts to verify fax numbers prior to faxing confidential and private information.
 - a. Employees need to periodically call to verify the intended recipient receives the faxes.
 - b. Management will keep fax machines in a reasonably secure location.
 - c. Employees will use required LADD cover sheet when faxing.
6. With prior consent of the person receiving services or their legal representative, a photograph of a person supported may be taken for the purposes of providing services to the person, determining the identity of the person or for education and training. The photograph, which includes still or video images, of the people supported may be taken with a program camera as long as that camera is kept locked and secured while not in use. The photograph is maintained in the person's record until discharge or until the purpose for which the photograph was taken no longer exists. In addition, some LADD publications such as brochures, newsletters and reports or the LADD website may include photographs of the people supported. This may only be done when a specific signed consent agreeing to the use of the photograph from the person or their legal representative has been obtained. Photographs of a person supported may be taken for purely personal or social purposes and shall be maintained as the person's private property not LADD property.
7. Video surveillance that includes recording of images is prohibited in keeping with the Michigan Mental Health Code MCL 330.1724.
8. All LADD office spaces are to remain locked while not in operation and all confidential information is to be locked in a secured location within the office. Individual workstations are to be maintained with all confidential information secured and computers logged off. Confidential information that is no longer in use or subject to destruction will be shredded by an approved contractor or at the point of production.
9. All IT assets are secured per the Technology Plan to include use of mobile device security software, email encryption software and the use of an approved IT asset destruction contractor.
10. Suspected violations of this policy can be reported to the Corporate Compliance Officer via the anonymous hotline, by email to corporatecompliance@laddinc.net or by submitting a Confidential Complaint. Reports may result in an investigation, assessment and notification to affected individual.

LADD

WE MAKE THE DIFFERENCE