



LIVING ALTERNATIVES FOR THE DEVELOPMENTALLY
DISABLED, INC.

COMPLIANCE AND ETHICS PROGRAM (CEP)

WE MAKE THE DIFFERENCE



INTRODUCTION

The LADD Compliance and Ethics Program (CEP) establishes the standards, policies and practices designed to provide guidance and communicate appropriate ethical and legal behavior for preventing fraud, abuse, waste and other unethical practices. All employees must commit to meeting the highest standards of ethical conduct. The CEP also exists to provide a process for the people we support, guardians, employees, personnel from other agencies, and community members to discuss or file complaints, grievances, violations, or problems with this organization or its employees, including Management, and to receive careful consideration and a prompt resolution.

The CEP is a collection of documents developed to help employees recognize and respond to some of the more sensitive and often problematic matters involved in conduct and ethics. The CEP specifies, where possible, actions and inactions that are contrary to and conflict with the duties and responsibilities of LADD employees. The CEP guides employees in conducting themselves and their work in a manner that reflects standards of behavior and professionalism as required by LADD.

At LADD the role of the Privacy Officer and the Security Officer are included in the responsibilities of the Corporate Compliance Officer (CCO). The CCO is responsible for the oversight of the CEP, all related policies, procedures, revisions, training, auditing, monitoring, investigations and record maintenance and release of information.

The CCO can be contacted at corporatecompliance@laddinc.net or by calling 1-855-607-1737.



LADD

WE MAKE THE DIFFERENCE



COMPLIANCE AND ETHICS PROGRAM (CEP)

TABLE OF CONTENTS

COMPLIANCE AND ETHICS PROGRAM

1 Introduction

Table of Contents
Compliance and Ethics Program Overview
HIPAA Overview

2 Privacy Practices

Privacy Notice
Acknowledgement of Receipt of Notice of Privacy Practices
Agreement to Receive Notice of Privacy Practices by Email
Documentation of Good Faith Effort

3 Confidentiality And Accessing Records

Policy on Responding to Subpoenas, Police, Media
Access to Records
Request for Records Release
HIPAA Security and Safeguard Policy
HIPAA Release of Confidential Information
Documentation of Disclosure of PHI

4 Business Associates

Business Associate Policy
Business Associate Contract

5 Breach Response

HIPAA Breach Response Policy
HIPAA Breach Assessment Worksheet
HIPAA Breach Notification Letter

6 Information and Technology Management Systems

Information Access Policy
Device and Media Control Policy
Workstation Access and Facility Security
Record Retention and Asset Management
Purge Grid
Non-Disclosure Agreement v1
Non-Disclosure Agreement v2
Confidentiality Agreement
Ex-Employee HIPAA Procedure

7 Employee Standards of Conduct

Standards of Conduct
Conflict of Interest- Code of Ethics Policy
Cell Phone and Texting Policy
Social Media Policy
Fund Raising Policy
Good Moral Character Policy
Harassment and Workplace Violence Policy

8 Corporate Standards of Conduct

Corporate Responsibility Policy
Corporate Giving Policy
Request for Corporate Assistance/Donation
Gifts, Bequests and Donations
Trademark Logo Use Policy
Auditing and Monitoring Policy
Responding to Audit Findings from External Monitoring Agencies
Compliance and Ethics Training Policy
Investigation Policy
Billing, Payment, and Personal Funds-Benefits Reconciliation Procedure- Office

9 Communication

Open Door Communication Policy
Whistleblower Policy
Complaint Reporting Policy
Complaint Reporting Form
Duty to Warn Policy

10 Closing



LADD

WE MAKE THE DIFFERENCE



COMPLIANCE AND ETHICS PROGRAM OVERVIEW

OVERVIEW

The LADD Compliance and Ethics Program (CEP) establishes the standards, policies and practices designed to provide guidance and communicate appropriate ethical and legal behavior for preventing fraud, abuse, waste and other unethical practices. All employees must commit to meeting the highest standards of ethical conduct. The CEP also exists to provide a process for the people we support, guardians, employees, personnel from other agencies, and community members to discuss or file complaints, grievances, violations, or problems with this organization or its employees, including Management, and to receive careful consideration and a prompt resolution.

The CEP is a collection of documents developed to help employees recognize and respond to some of the more sensitive and often problematic matters involved in conduct and ethics. The CEP specifies, where possible, actions and inactions that are contrary to and conflict with the duties and responsibilities of LADD employees. The CEP guides employees in conducting themselves and their work in a manner that reflects standards of behavior and professionalism as required by LADD.

Additional guidance on matters of conduct is provided in the Employee Handbook Code of Conduct. All employees of LADD are expected to follow ethical practices which means working and providing care in a way that is honest, legal and respectful of others; and reflects the Mission, Vision and Values of LADD This is a requirement for employment.

LADD standards for excellence are based on honesty, integrity, fairness, respect, trust, responsibility, and accountability in operations, governance, human resources, financial management, community supports and fundraising.

CEP ELEMENTS

The CEP is based on the seven fundamental elements of an effective compliance program and also includes information related to HIPAA compliance. The CEP contains policies, procedures and forms related to compliance, employee conduct and the confidentiality of information. In order to organize and simplify the information contained in the CEP it is structured around each of the seven elements as follows;

- I. Designating a corporate compliance officer and compliance committee.
- II. Implementing written policies, procedures and standards of conduct.
- III. Conducting effective training and education.
- IV. Developing effective lines of communication.
- V. Conducting internal monitoring and auditing.
- VI. Enforcing standards through well-publicized disciplinary guidelines.
- VII. Responding promptly to detected offenses and undertaking corrective action.

SECTION I - Designating a Compliance Officer (includes the responsibilities of Privacy Officer and Security Officer) and a Compliance Committee

At LADD the role of the Privacy Officer and the Security Officer are included in the responsibilities of the Corporate Compliance Officer (CCO). The CCO is responsible for the oversight of the CEP, all related policies, procedures, revisions, training, auditing, monitoring, investigations and record maintenance and release of information. The CCO must be knowledgeable in all applicable standards and engage in ongoing training and education to prevent improper conduct, illegal activities, unethical behavior and improper record and asset management. The CCO has a direct reporting responsibility to the Board of Directors and the Executive Director so there is no actual or perceived conflict in investigating and reporting issues. The CCO has a job description and responsibilities specific to their position at LADD Inc. which includes;

- Providing ongoing training in compliance related matters, HIPAA/HITECH, Breach of Confidential Information, DRA, FCA including Fraud, Waste and Abuse and Whistleblowers to all employees.
- Collaborates with other departments to direct compliance issues to appropriate departments for investigation and resolution.
- Responds to alleged violations of rules, regulations, policies, procedures, and Standards of Conduct by evaluating or recommending the initiation of investigative procedures. Develops and oversees a system for uniform handling of such violations.

- Oversight of the Business Associate Contracting system.
- Prevention, detection and response to security events including breaches.
- Direct the release of information process.

The CCO is easily accessible to all stakeholders. Contact information for questions or filing a complaint is available;

- On the LADD Website and People Supported Website
- Available in all Programs
- Included in online training initially and annually
- Included in the Service Information Packets

Complaints may be made openly or anonymously to the CCO and will not result in retaliation by LADD or its employees. All stakeholders, including employees of LADD must immediately report to the CCO, any suspicion of fraud, waste, abuse or violation of confidentiality as it relates to protected health information.

LADD maintains a Compliance Committee/Steering Committee that consists of individuals within the corporation who are in a position to affect the culture of the organization, knowledgeable in the operation of the organization and possess a diverse background/area of specialty. The CCO is the chairperson of the committee and utilizes the committee's expertise to assist with implementation of the CEP. The Committee serves as a resource to the CCO to assist with;

- Communicating the corporation's practices
- Assessing the corporation's risk
- Developing policy and procedure
- Taking corrective action

In addition, the role of the entire team of leadership at LADD is to establish and maintain a culture of compliance and ethical conduct. LADD employees in Management and leadership positions are expected to:

- Serve as Compliance Liaisons at locations where LADD provides staffing supports. Compliance Liaisons are responsible for bringing compliance issues to the CCO, training related to corrective actions and facilitating stakeholder questions/concerns.
- Ensure those they supervise have information and are educated regarding applicable laws, regulations, and policies and legal requirements pertinent to their function.
- Inform all staff they supervise that strict compliance with policies and regulation is a condition of employment and violation will result in disciplinary action up to and including separation.
- Encourage the reporting and discussion of concerns related to legal and ethical practice; insure adequate follow up to concerns.
- Ensure that business practices do not compromise ethical behavior or our core values.

SECTION II – Implementing Policies, Procedures and Standards of Conduct

The LADD Employee Handbook Code of Conduct, the LADD Directory and Management Manual contain several policies and procedures that provide standards and guidance for employees and business operations. They are designed to help employees understand their rights and responsibilities, to work more efficiently and to provide care in an ethical way. These resources are readily accessible on line for employees. It is the expectation that all LADD employees complete their job in an ethical manner with the best interest of LADD in mind at all times.

Privacy Notice

Access to Records

Business Associates Policy

HIPAA Safeguard and Security Policy

Device and Media Control Policy

HIPAA Breach Response Policy

Information Access Policy

Record Retention and Asset Management

Workstation Access and Facility Security

Social Media Policy

Trademark and Logo Use Policy

Cell Phone and Texting Policy
Corporate Responsibility Policy
Corporate Giving Policy
Gifts, Bequests and Donation Policy
Fund Raising Policy
Billing, Payment and Personal Funds-Benefits Reconciliation Procedure- Office
Conflict of Interest-Code of Ethics Policy
Standards of Conduct
Good Moral Character Policy

SECTION III. Conducting Effective Training and Education

All potential employees receive a copy of the LADD Mission, Vision and Values at the initial interview in an effort to communicate to them the principles that guide the organization and the behavior that is expected if they are to be employed.

During new hire orientation employees are provided with;

- An explanation regarding how to access the Employee Handbook Code of Conduct as well as how to retrieve and review full policies and procedures.
- Receive training regarding on line access to the CEP and how to review/search information.
- Receive training regarding the CEP and related topics such as the Deficit Reduction Act, Whistleblowers, HIPAA and HITECH.

Annually, all employees receive training regarding the CEP and related topics such as the Deficit Reduction Act, Whistleblowers, HIPAA and HITECH.

When people supported and Guardians begin services with LADD they are provided with information about accessing the CEP on the LADD website.

Compliance and Ethics Training Policy

SECTION IV. Developing Effective Lines of Communication

In order to provide the highest level of services and adhere to the LADD Mission, Vision and Values; employees are expected to be honest ethical and act with integrity. Standing in Truth is a core competency for all LADD employees. Being of Good Moral Character is a job essential requirement to remain employed and is written in all job descriptions. Employees are expected to provide high quality care to vulnerable adults and children. In doing so, they must be honest, speak the truth, act and speak with integrity and positive intent. The people we support rely on employees for their physical and emotional well-being. They must act with kindness and compassion, communicate with positive intent, and immediately correct and report any wrong doing. Employees who observe or are aware of violations of LADD policies or procedures must report them to Management and/or the Corporate Compliance Officer immediately. Employees are required to ensure the rights of the people we support and keep them safe at all times.

Complaint Reporting Policy

Open Door Communication Policy

Whistleblower Policy

Duty to Warn Policy

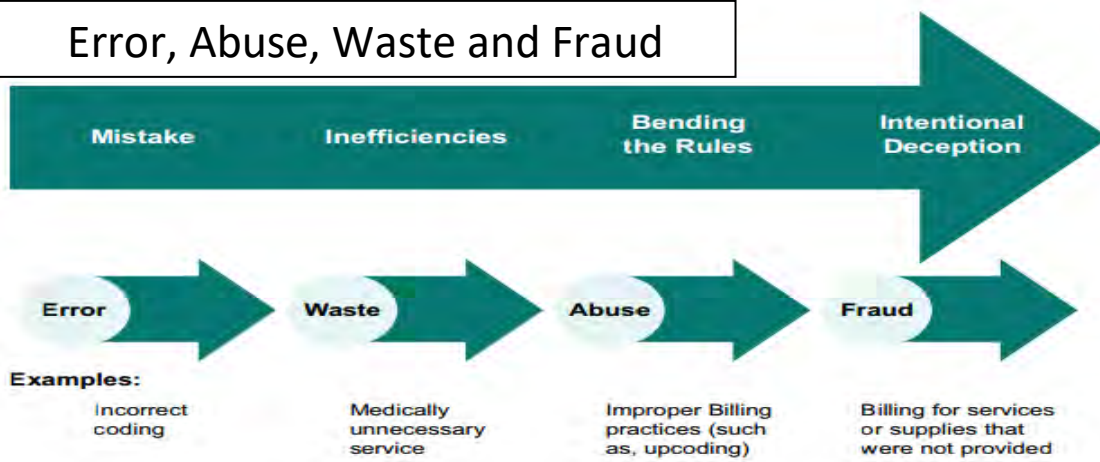
Policy on Responding to Subpoenas, Police and Media

Harassment and Workplace Violence Policy

SECTION V. Conducting Internal Monitoring and Auditing

LADD is a non-profit corporation dedicated to making the difference in people's lives. LADD must act ethically when establishing expectations of behavior, character, and conduct; and maintain the distinction between right and wrong, and eliminating fraud, waste and abuse. LADD is responsible for achieving results through improved quality of life.

Error, Abuse, Waste and Fraud



Auditing and Monitoring Policy

Audit- Responding to Audit Findings from External Monitoring Agencies

Billing, Payment and Personal Funds/Benefits Reconciliation Procedure

SECTION VI. Enforcing Standards Through Well-Publicized Disciplinary Guidelines

Employees receive direction on accessing the Employee Handbook Code of Conduct at the time of hire and training throughout their employment regarding policies/procedures that establish standards for disciplinary action and/or possible separation from employment. Personnel matters are confidential by nature and as such, most often, violators of the CEP will not have publicized disciplinary action. However, violations of the CEP will be addressed through timely and consistent disciplinary action which could include separation from employment.

All CEP violations are immediately corrected, including any additional education and training that is necessary for prevention. Education and training are primarily addressed during semi or annual training or through in person meeting/trainings in all programs.

In most cases, remedial actions are designed to improve the performance of LADD employees. Management will identify the exact nature of and need for remedial action in collaboration with Administration and/or CCO.

SECTION VII. Responding Promptly to Detected Offenses and Undertaking Corrective Action

Failure to comply with the LADD CEP or the laws and/or regulations applicable to federally funded behavioral health care programs, Home help services, or any program of training, counseling or remedial action which an employee has been required to undertake, may result in discipline up to and including separation from employment or association with LADD.

In cases of intentional misconduct, repeated violations, or after documented remediation(s) have failed to correct the problem, LADD may initiate corrective or disciplinary actions. The initiation of corrective or disciplinary action by LADD does not preclude or replace any criminal proceedings that may be taken by the appropriate legal authority.

Investigation Policy

CLOSING

LADD is committed to all elements of the CEP and continuously reviews and revises policies, procedures and practices to remain compliant with all laws, regulations and standards of best practice. LADD is committed to standards for ethical practices concerning staff, Management and all operations of LADD. Inclusive in these is the expectation that support services are provided responsibly, fairly and with awareness of the surrounding community and provide services consistent with LADD Mission, Vision and Values.



HIPAA OVERVIEW

The LADD CEP establishes standards and policies that communicate appropriate ethical and legal behavior to protect the confidential and private information belonging to the people supported. The CEP provides the basis for how information is created, stored, transmitted, accessed and destroyed in a way that prevents unethical and improper practices and ensures all employees are striving to meet the highest performance standards and ethical conduct. The CEP provides a process for the people we support, families, guardians and personnel from other entities to obtain information and to discuss, file complaints or grievances relative to the aforementioned information and to receive careful consideration and a prompt resolution.

The Health Insurance Portability and Accountability Act (HIPAA) is divided into three sections; the Privacy Rule, Breach Notification and the Security Rule.

1. The Privacy Rule defines:

- How LADD may use PHI.
- Under what conditions LADD can disclose PHI.
- Individual rights related to PHI.
- How LADD will notify individuals of those rights.
- How LADD works with an individual to exercise those rights.

2. Breach Notification Rule defines:

- Steps LADD must take to assess if a breach of PHI occurred.
- Steps LADD is to take if a breach has been discovered.

3. The Security Rule defines:

- Steps LADD takes to prevent unauthorized access to **electronic** PHI.
- How LADD can ensure the integrity of information.
- How LADD can ensure that information remains available.

Privacy Rule

1. Protected Health Information (PHI) is individually identifiable health information that is transmitted by electronic media, maintained in electronic form or that is maintained or transmitted in any other form. Info is PHI if it relates to:

- Physical/mental health or condition of an individual
- Provision of health care
- Payment for provision of health care

A simplified method to decide if information is PHI is to look at the rules that apply to protecting individually identifiable information (De-identification using Safe Harbor methodology). The following identifiers for individual or of relatives, employers, or household members of the individual must be de-identified and therefore are considered PHI:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
 - The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
 - The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet Protocol (IP) addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying number, characteristic, or code, except as permitted under special circumstances to assist with re-identification.
- Certificate/license numbers

A deceased person has HIPAA protection for 50 years from the date of death.

Personnel records are not subject to HIPAA standards and the information contained within the record is not considered PHI as it relates to HIPAA i.e. FMLA, sick leave, worker's compensation. Personnel records do contain confidential information that is regulated by the Office for Civil Rights, Equal Employment Opportunity Commission and Department of Labor and the Human Resource Department should review and implement systems to secure confidential employee information.

2. Use and Disclosure of PHI is permitted according to these broad categories, as applicable to LADD's operations;

- Treatment, Payment, and Health Care Operations
 - Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.
 - Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
 - Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying PHI, creating a limited data set, and certain fundraising for the benefit of the covered entity.
- Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.
 - For Notification and Other Purposes- LADD may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, PHI directly

relevant to that person's involvement in the individual's care or payment for care. This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose PHI for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. **In addition, PHI may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.**

- Public Interest and Benefit Activities permit use and disclosure of PHI, without an individual's authorization or permission, for 12 national priority purposes.
 - Required by Law- LADD may use and disclose PHI without individual authorization as required by law (including by statute, regulation, or court orders).
 - Public Health Activities. LADD may disclose PHI to public health authorities
 - Victims of Abuse, Neglect or Domestic Violence- In certain circumstances may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.
 - Health Oversight Activities- LADD may disclose PHI to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations.
 - Judicial and Administrative Proceedings- May disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.
 - Law Enforcement Purposes- LADD may disclose PHI to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that PHI is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.
 - Decedents- LADD may disclose PHI to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.
 - Cadaveric Organ, Eye, or Tissue Donation- LADD may use or disclose PHI to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.
 - Research- Under some circumstances disclosures for research may be permissible although it is not likely to occur at LADD.
 - Serious Threat to Health or Safety- LADD may disclose PHI that is believed to be necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.
 - Essential Government Functions- An authorization is not required to use or disclose PHI for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.
 - Workers' Compensation- LADD may disclose PHI as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

3. Minimum Necessary standard is based on the concept PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. LADD must take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following;

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made following an individual's authorization.
- Uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.
- Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

4. Business Associates (BA) are directly liable for compliance with HIPAA standards and have a shared liability with LADD to ensure standards are adhered to. A BA is defined as an individual or entity that;

- Creates, receives, maintains or transmits PHI with LADD.
- Not part of the LADD workforce (on payroll).
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

A covered entity can be the BA of another covered entity.

The Privacy Rule allows LADD to disclose PHI to BA if LADD obtains satisfactory assurances through a Business Associate Contract (BAC) that the BA will use the information only for the purposes for which it was engaged, will safeguard the information from misuse and will help LADD to remain compliant with the standards of the Privacy Rule.

A BAC is NOT required with an individual or entity (i.e. janitorial service or electrician) whose functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all.

5. HITECH (Health Information Technology for Economic and Clinical Health Act) is the penalty portion of Privacy Rule. In order to avoid the possibility of penalties the following can be taken into consideration;

- Must be able to demonstrate LADD did not willfully neglect a standard.
- Must be able to demonstrate LADD did not know, and by reasonable diligence would not know a standard was violated.

HITECH has a four-tiered penalty arrangement that consists of increasing levels of fines based on the severity of the violation. Criminal penalties can be applied as well. The following grid provides a simplified interpretation of the penalty stages;

- **Unknowning-** The covered entity or business associate did not know and reasonably should not have known of the violation.
- **Reasonable Cause-** The covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but the covered entity or business associate did not act with willful neglect.
- **Willful Neglect, Corrected-** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA. However, the covered entity or business associate corrected the violation within 30 days of discovery.
- **Willful Neglect, Uncorrected-** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation within 30 days of discovery.

The corresponding tiers of Civil Monetary Penalties (CMP) relating to each level of liability are as follows:

Violation Category	Each Violation	Total CMP for Violations of an Identical Provision in a Calendar Year
Unknowing	\$100	\$25,000
Reasonable Cause	\$1,000	\$100,000
Willful Neglect, Corrected	\$10,000	\$250,000
Willful Neglect, Not Corrected	At least \$50,000	\$1,500,000

Breach Notification Rule

1. Unsecured Protected Health Information

LADD and BA must only provide the required notifications if the breach involved Unsecured Protected Health Information (UPHI). UPHI is PHI that has **NOT** been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS as follows;

- Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption). and such confidential process or key that might enable decryption has not been breached.
- The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
 - Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. **Redaction** is specifically excluded as a means of data destruction.
 - Electronic media have been cleared, purged, or destroyed such that the PHI cannot be retrieved.

2. Breach Assessment is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless LADD or BA demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

There are three exceptions to the definition of “breach.”

- The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of LADD or BA, if such acquisition, access, or use was made in good faith and within the scope of authority.
- The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a LADD or BA to another person authorized to access PHI at the LADD or BA, or organized health care arrangement in which LADD participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception applies if LADD or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

3. Notification - LADD is required to and will notify people supported, and if applicable their guardian and the contract agency if it is determined there has been a breach of their PHI. LADD will take steps to mitigate risks identified with the breach which could include monitoring by an identity theft and fraud detection monitoring service.

LADD must notify affected individuals following the discovery of a breach of UPHI as follows;

- Must provide individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
- If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- Must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.
- Must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include;
 - A brief description of the breach.
 - A description of the types of information that were involved in the breach.
 - The steps affected individuals should take to protect themselves from potential harm.
 - A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches.
 - Contact information regarding questions.
- LADD must maintain proof demonstrating that all required notifications have been provided or that a use or disclosure of UPHI did not constitute a breach.

If a breach of UPHI affects **fewer** than 500 individuals, LADD must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered and may notify sooner at LADD's discretion. The following must occur;

- A separate notice must be completed for each breach incident.
- Notice must be submitted electronically by clicking on the link below and completing all of the fields of the breach notification form.

Security Rule

1. The Security Rule establishes national standards to protect individuals' Electronic Protected Health Information (EPHI) that is created, received, used, or maintained at LADD. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of EPHI. PHI is considered EPHI if it is maintained or stored in an electronic format. The Security Rule is divided into three sections:

- Administrative – training, auditing, reporting
- Physical – locked doors, screen protectors
- Technical – login passwords, wireless passwords

Each section consists of multiple standards which can be subdivided as needed. If the Standard is a standalone item it is deemed self-explanatory and is **required**. However if a broader concept is communicated as part of the Standard it is subdivided and referred to as an Implementation Specification. As stated Implementation Specifications are sub-categories of a Standard and are meant to communicate a concept necessary to meet the Standard. Implementation Specifications are either **required** or **addressable** (or recommended). When a standard is **addressable** it must be determined if it is reasonable for LADD to complete as part of best practice.

2. Electronic Protected Health Information is looked at differently than PHI. The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called PHI, as explained in the Privacy Rule portion. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information LADD creates, receives, maintains or transmits in electronic form. The Security Rule calls this information EPHI. The Security Rule does not apply to PHI transmitted orally or in writing.

3. Within the Administrative portion of the Security rule is the requirement that covered entities must have a **Disaster Recovery Plan (DRP)** and an **Emergency Mode of Operation Plan (EMOP)**. The purpose of each plan is make sure ePHI is available in the event of a disaster like fire, vandalism, natural disaster or system failure and that operations will continue and ePHI will continue to be supported and available. At LADD a DRP is completed annually and updated with current practices. The DRP is reviewed by the Steering Committee as part of Strategic Planning. The DRP outlines how ePHI will continue to be available and supported. LADD has a Corporate Emergency Plan that is reviewed and maintained by the Emergency Management Committee. The Corporate Emergency Plan addresses several scenarios and how to plan and respond in those situations related to EMOP. Between the LADD DRP and Corporate Emergency Plan this standard is met.

Closing

As a covered entity, LADD must be in full compliance with all standards contained within HIPAA relative to the people supported and their PHI. LADD recognizes that employee information, including information contained in the personnel file is sensitive and must remain confidential utilizing the same methods and standards outlined in HIPAA whenever applicable. Therefore, all policies and procedures contained within the CEP apply equally to people supported and employees.





PRIVACY PRACTICES

Every person supported by LADD must have their personal and confidential information protected from unauthorized use. The Notice of Privacy Practices outlines the person's rights and LADD's responsibilities and obligations regarding the person's information.



LADD

WE MAKE THE DIFFERENCE

Notice of Privacy Practices For Living Alternatives for the Developmentally Disabled, Inc.

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY

◆ Understanding Your Health Record/ Information

When receiving services from L.A.D.D., Inc. if another health care provider contacts us concerning your medical needs or history, documentation of the contact is kept in the program. Sometimes a disclosure is made that is outside of treatment, payment or healthcare operations or for which an authorization is given, documentation of such disclosures are kept in the office by the Corporate Compliance Officer. In this "Notice of Privacy Practices," we shall refer to the information contained in your record as your "health information." This term shall have the same meaning as "protected health information" defined in the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

Your Health Information Rights- Within the limits provided by federal and state law, you have the right to:

- Request restrictions on certain uses and disclosures of your health information.
- Receive confidential communications of your health information. You may request that we communicate with you about your health information by alternative means or at an alternative location.
- Restrict disclosures of your health information to a health plan with respect to health care for which you have paid out of pocket in full.
- Inspect and obtain a copy of your health information, except with regard to psychotherapy notes or information compiled in reasonable anticipation of certain civil, criminal or administrative proceedings.
- Request an amendment to your health information that we have created, except with regard to those portions of your health information that you are precluded from inspecting and copying as set forth above.
- Obtain an accounting of certain disclosures of your health information.
- Receive a paper copy of this Notice in addition to any electronic copy you may receive.

You may exercise any of the above rights by submitting a signed letter detailing your request and mailing or delivering the letter to our Privacy Officer/Corporate Compliance Officer. At L.A.D.D., Inc. our Corporate Compliance Officer serves in the role of Privacy Officer.

However, we encourage you to call first so that we can help you be as specific as possible with your request. We will promptly provide you with any forms needed to process your request.

Unless you tell us otherwise in writing, we may contact you by either telephone or by mail at either your home or your workplace. At either location, we may leave messages for you on the answering machine or voice mail. If you want to request we communicate to you in a certain way or at a certain location see the point above regarding confidential communication.

Our Responsibilities- This Office is required by law to:

- Maintain the privacy of your health information;
- Provide you with this Notice of our legal duties and privacy practices with respect to health information we collect and maintain about you;
- Abide by the terms of this Notice, currently in effect, and as amended from time to time;
- Notify you if we are unable to honor your request to restrict a use or disclosure of, or to amend, your health information; and
- Accommodate reasonable requests you may have to communicate your health information by alternative means or at alternative locations.
- Notify you when there has been a breach of your health information as required under Breach Notification standards of HIPAA. Such notice will be provided without unreasonable delay within 60 days of the date we discover the breach.

We reserve the right to change our privacy practices and to make the new provisions effective for all of your health information we already have, as well as any health information we receive or create in the future. Should our privacy practices change, we will post a copy of the revised Notice in our programs, which indicates the effective date of the amended Notice. Each time you visit our program you will be able to view any revisions of the privacy notice posted in each program you may also have a copy of our current Notice of Privacy Practices upon your request. Our Notice of Privacy Practices are also available at our website.

If a use or disclosure of your health information is not permitted under law without a written authorization, we will not use or disclose your health information without that written authorization. You may at any time revoke a written authorization in writing, except to the extent that we have already taken action in reliance of your authorization.

If you have questions and would like additional information concerning this Notice, please call our Privacy Officer at 269-782-0654

If you believe that we have violated any of your privacy rights, you may file a written complaint with our Corporate Compliance Officer, or mail your written complaint to:

Corporate Compliance
L.A.D.D., Inc.
300 Whitney Street
Dowagiac, MI 49047
Anonymous Reporting 1-855-607-1737

You may also file your complaint with the Secretary of Health and Human Services. There will be no penalty or retaliation for filing a complaint. Complaints filed with the Secretary of Health and Human Services should be addressed to:

Office of Civil Rights
U.S. Department of Health and Human Services,
200 Independence Avenue SW,
Washington, D.C. 20201
Or complaints may also be filed at <http://www.hhs.gov/ocr>

◆ Examples of Uses and Disclosures for Treatment, Payment and Health Operations

The following are examples of uses and disclosures of your health information which are permitted by law: We use and disclose health information about you for a number of different purposes. We may disclose this information electronically, password protected if necessary. Each of those purposes is described below:

We will use your health information for treatment. We will use your health information to provide, coordinate or manage your health care and related services to you. As a part of these services minimum necessary information may be released for the purpose of building natural supports, community supports, and acquiring daily living skills. Any of our staff involved in your care will have access to your health information. We may also provide your health information to other health care providers who become involved in your care; including Contract Agencies to assist them in providing services to you. Similarly, we may refer you to another provider for services and as a part of the referral share health information about you with that provider. In the course of our daily operations if one person's services/treatment are affected by actions of another individual than either individual's minimum necessary information may be released. However, we will not disclose psychotherapy notes to health **care providers who are not part of our practice unless we have your written authorization to do so.**

We will use your health information for payment. Your health plan or health insurer will require certain information about your condition and the services you receive from us, before payment will be made. Accordingly, for billing purposes, we may disclose your health information to your health plan **or** health insurer. We also may disclose health information to your health plan or health insurer when they require preauthorization of a recommended procedure. We also may need to provide your insurance company or a government program, such as Medicare or Medicaid, with

information about your medical condition and the health care you need to receive to obtain determine if you are covered by that insurance or program.

We will use your health information for regular health care operations. We may use and disclose medical information about you for our own health care operations. These are necessary for us to operate L.A.D.D., Inc. and to maintain quality health care for the people we serve. For example, we may use health information about you to review the services we provide and the performance of our employees in caring for you. We may disclose health information about you to train our staff, and volunteers working at L.A.D.D. Inc., We also may use the information to study ways to more efficiently manage our organization. This information may also be released to accrediting agencies in an effort to continually improve the quality and effectiveness of our services.

◆ **Additional Uses and Disclosures**

Business Associates: Certain of our business operations may be performed by other businesses. We refer to these companies as "business associates." In order for these business associates to perform the required service (billing, accounting services, etc.), we may need to disclose your health information to them so that they can perform the job we've asked them to do. To protect you, we require our business associates to appropriately safeguard your health information.

Communication with Persons Involved in Your Care: We may disclose to a family member, other close relative, a close personal friend, or any other person identified by you, health information about you that is directly relevant to that person's involvement with your care. Please note in your plan of service if there is someone specific you do not want information disclosed to about you. If you are incapacitated, or involved in an emergency, we may use or make disclosures of your health information that we believe in our professional judgment are in your best interests, but only to the extent that such health information is directly relevant to the recipients' involvement in your care.

Required by Law: We may use or disclose your health information to the extent that such use or disclosure is required by law and is limited to the relevant requirements of such law.

Public Health, Health Oversight and the Food and Drug Administration (FDA): As required by law, we may disclose your health information to public health or legal authorities charged with preventing or controlling disease, injury, or disability. We may also be required by law to disclose your health information to health oversight agencies responsible for regulating the health care system, government benefit programs, and civil rights laws, so that they may conduct, among other things, audits, investigations, and inspections. For the purpose of activities relating to the quality, safety or effectiveness of a FDA-regulated product or activity, we may disclose to the FDA your health information relating to adverse events with drugs, supplements, and other products, as well as information needed to enable product recalls, repairs, or replacements.

Victims of Abuse, Neglect or Domestic Violence: If we reasonably believe that you are the victim of abuse, neglect or domestic violence, we may disclose your health information to a governmental authority responsible for receiving these types of reports, to the extent the disclosure is required by law, or you agree to the disclosure. If the disclosure is authorized by law, but not required, we may disclose your information if we determine that disclosure is necessary to prevent serious harm to you or others.

Judicial and Administrative Proceedings: If you are involved in a judicial or administrative proceeding we may, in response to an order of a court or administrative tribunal, or in response to a subpoena, discovery request, or other lawful process, disclose the specific portions of your health information that are requested. If the subpoena, discovery request or other lawful process is not accompanied by a court or administrative tribunal order, we may disclose your health information only after we are assured that reasonable efforts have been made to notify you of the request, and the time for you to raise objections to the request has expired, or reasonable efforts have been made by the requester to seek a protective order concerning the requested health information.

Law Enforcement: We may disclose your health information to a law enforcement official for law enforcement purposes as required by law, a court ordered subpoena or summons, a grand jury subpoena or summons, or an administrative subpoena or summons, under certain circumstances.

In specific situations, the law also permits us to disclose limited pieces of your health information, when the information is needed by law enforcement officials to: 1) identify a suspect, fugitive, material witness, or missing person; 2) identify a victim of a crime; 3) alert law enforcement officials concerning your death; 4) notify law enforcement officials when a crime has been committed on our premises; or 5) in an emergency, when necessary to alert law enforcement officials about a crime, its location, or the identity of a perpetrator.

Coroners Medical Examiners and Funeral Directors- We may disclose your health information to a coroner or medical examiner for the purpose of identifying you upon your passing, or to determine a cause of death. We may also disclose your health information to your funeral director if needed to complete his or her authorized duties.

Cadaver Organ, Eye or Tissue Donation: If you are an organ donor, we may release your health information to organizations that procure, bank or transplant organs for the purpose of facilitating organ, eye or tissue donation and transplantation.

Research: We may disclose your health information to researchers when their research has been approved by an institutional review board or privacy board that has reviewed the research proposal and established protocols to ensure the privacy of your health information, thereby meeting the requirements under HIPAA.

Avert a Serious Threat to Health or Safety: Consistent with applicable law and standards of ethical conduct, we may, in limited circumstances, use or disclose your health information if we, in good faith, believe such use or disclosure is necessary to prevent or lessen a serious and imminent threat to health or safety of a person or the public.

National Security and Presidential Protective Services: We may disclose your health information to authorized federal officials for the conduct of lawful intelligence and national security activities, as well as the provision of protective services to the President and other protected individuals.

Inmates and Individuals in Custody: If you are an inmate or otherwise in custody, we may disclose your health information to the correctional facility or law enforcement official having lawful custody of you.

Workers' Compensation: We may disclose your health information to the extent authorized and necessary to comply with laws relating to workers' compensation or other similar programs established by law.

Disaster Relief: We may use or disclose your information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. This will be done to coordinate with those entities in notifying a family member, other relative, close personal friend, or other person identified by you, of your location, general condition or death.

Proof of Immunization: We may use or disclose your information to a school about you if you are a student or perspective student of the school. The information is limited to proof of immunization. This will occur if the school is required by law to have proof of immunization prior to admittance and we obtain your agreement.

Fund Raising and Marketing: As a tax-exempt organization, we may solicit and accept contributions. Unless you instruct us otherwise, we may use your contact and demographic information, as well as dates of service and outcome information for the purpose of raising funds. You have the right to opt out of fundraising activities. Any marketing activities that include the use of you information will include your agreement.

Our Pledge

We endeavor to provide you with the highest level of care while protecting the privacy of your health information. If you have any questions, comments, or concerns regarding the policies set forth above, please do not hesitate to discuss such matters with our Corporate Compliance Officer.

Living Alternatives for the Developmentally Disabled, Inc.

(L.A.D.D., Inc.)

www.Laddinc.net

300 Whitney Street

Dowagiac, MI 49047

269-782-0654

Fax 269-782-3828

Original 03/14/03,

Revised 12/7/06, 12/7/10, 1/16/12, 11/28/12, 9/11/13, 1/1/16, 1/1/19



RECEIPT OF NOTICE OF PRIVACY PRACTICES ACKNOWLEDGEMENT

By signing this Acknowledgement of Receipt of Notice of Privacy Practices I am acknowledging that I have received a copy of the LADD Notice of Privacy Practices. Furthermore, I understand the LADD Notice of Privacy Practices is available online at the LADD website and/or available to me at any time at any LADD facility by asking for a copy. I understand that I can also request a copy of the LADD Inc. Notice of Privacy Practices by contacting any LADD office and/or the Corporate Compliance Officer at 269-782-0654. In the event of a breach of my protected health information, I understand and acknowledge notification to me may be done in writing or email.

Print Person's Name

Person's Signature

Date

Guardian's Signature

Date

LADD

WE MAKE THE DIFFERENCE



AGREEMENT TO RECEIVE NOTICE OF PRIVACY PRACTICES BY EMAIL ACKNOWLEDGEMENT

Please send me LADD's Notice of Privacy Practices by e-mail. In addition, in the event of a breach of my protected health information I understand and acknowledge notification to me may be done by email.
My e-mail address is:

Print Person's Name

Person's Signature

Date

Guardian's Signature

Date



LADD

WE MAKE THE DIFFERENCE



DOCUMENTATION OF GOOD FAITH EFFORT

To Obtain Written Acknowledgment of the Receipt of Notice of Privacy Practices

Name of Individual: _____

(1) Effort to Obtain Written Acknowledgment of Notice of Privacy Practices:

(2) Reason Why the Written Acknowledgment Was Not Obtained:

LADD

WE MAKE THE DIFFERENCE

Corporate Compliance Officer

Date



CONFIDENTIALITY AND ACCESS TO RECORDS

Under certain circumstances information may be shared with other individuals. In these circumstances proper procedures must be followed and every employee is responsible to know and follow procedures. If an employee has a question regarding the correct way to share information they must review their questions with a member of management immediately, before sharing the information.



LADD

WE MAKE THE DIFFERENCE



POLICY ON RESPONDING TO SUBPEONAS, POLICE AND MEDIA

PURPOSE

To establish guidelines for management and staff to follow in responding to subpoenas, requests for information, police investigations and media requests for information.

SCOPE

This policy applies to all employees of LADD.

POLICY

The Board of Directors and management of LADD are committed to operating in accordance with responsible business practices and legal requirements and to providing methods for which employees will comply with all lawfully executed subpoenas, search warrants or other types of legal directives as well as requests for information from the media.

STANDARDS AND DEFINITIONS

None

PROCEDURE

In the interest of orderly, consistent management of the information released for legal proceedings or to the media, the following procedures are in effect:

LAW ENFORCEMENT

1. Employees must report to their supervisor any contact by law enforcement at the time the contact is made and prior to disclosing confidential information.
2. The supervisor will contact the Regional Director for further guidance and authorization to disclose information to law enforcement.
3. If information is to be disclosed the Regional Director will email the details of the disclosure to the Executive Director or CCO who will enter the information in the Disclosure database.
4. Once authorized employees may disclose protected health information in response to a law enforcement request for such information about an individual for the following reasons:
 - as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests
 - to identify or locate a suspect, fugitive, material witness, or missing person
 - in response to a law enforcement official's request for information about a victim or suspected victim of a crime
 - to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death
 - when a covered entity believes that protected health information is evidence of a crime that occurred on its premises
 - by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime
3. if the information is needed to identify or apprehend an escapee or violent criminal ***Serious Threat to Health or Safety***. Employees may disclose protected health information they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).
4. Any time information is released it is to be documented and the guardian is to be notified.

SUBPOENAS, SEARCH WARRANTS OR OTHER LEGAL DIRECTIVES

1. In the event that LADD employees are presented with a subpoena, search warrant or other type of legal directive that is related to LADD they must immediately contact their direct supervisor who will contact the Regional Director. Employees are to ask the person presenting this information to present them with proper identification and to remain outside of the location until they can contact their direct Supervisor for further direction; employees are not to allow the person into the program.
2. Administration will review the identification to make certain the individuals conducting the search are valid members of a law enforcement agency and that the search is authorized by a court of law.
3. The law enforcement officials should then be permitted to conduct the search as duly authorized by the search warrant.
4. In the event that the designated member of Administration is unavailable or is determined to have a conflict of interest regarding the subpoena, search warrant or other legal directive, the matter should be referred to the Executive Director or CCO.
5. It is the policy of LADD to assess the validity and scope of the subpoena, search warrant or other legal directive to ensure that the person supported, corporate or employee's privacy and confidentiality rights are not violated.
6. When appropriate, subpoenas for consumer records may be referred to the designated mental health agency, who is the holder of the record per the state Mental Health Code.
7. If it is determined that the subpoena, search warrant or other legal action is related to a potential quality of care issue or other potential violation of corporate policy, Administration shall initiate an investigation and recommend whether any interim action is appropriate as long as this investigation does not interfere with law enforcement officials.
8. Any written court or legal documents delivered to a work location must not be opened and sent immediately to the CCO at the LADD office.

MEDIA

1. Any employee or management personnel who are contacted by the media (newspaper reporter, TV reporter, etc.) must direct the media to the Executive Director or CCO.
2. Employees will not give out any location, employee, person supported or Management telephone numbers to a member of the media. They will inform the member of the media that they will have someone get back with them as soon as possible. Employees will write down their information and telephone number to provide to a member of Management.
3. At the time of contact, employees or Management must immediately inform their direct supervisor who will contact a member of Administration.
4. Employees must be professional and courteous to the media contact.
5. Use the following as the basis for a response. "I am currently providing support services and in order to provide the care that is needed I cannot answer your questions. If you will give me your name and number I will have someone get back with you as quick as possible."

ADMINISTRATION

1. Administration is to assume full responsibility for overseeing and complying with the legal matters addressed in this policy or the contact made by the media. When possible the Executive Director or CCO will be contacted for further direction.
2. The Executive Director in conjunction with the CCO may seek legal counsel.



ACCESS TO RECORDS POLICY

PURPOSE

To establish a policy through which the employees, individuals we support and/or guardians may have access to their personnel records or protected health information.

SCOPE

This applies to all employees of LADD and individuals served by LADD.

POLICY

It is the policy of LADD to follow HIPAA standards and provide for the person supported and guardians to access, inspect and obtain a copy of their information; and to approve disclosures and have an accounting of disclosures. This policy also covers employees and how they can access their personnel records.

STANDARDS AND DEFINITIONS:

Individual Records Sign Out – Found in the HIPAA log located at each location and is used to document when a staff removes a hard copy of the person's record for an appointment.

Disclosure Authorization – LADD requires a release, signed by the person or their guardian, giving permission for LADD to share information regarding the person as directed in the disclosure (called Release of Confidential Information, HIPAA Disclosure). This document is sometimes referred to as a release and can include information specific to individual circumstances.

The State of Michigan requires a specific disclosure authorization format when releasing information related to behavioral health called the DHS 3927 Consent to Share Behavioral Health Information for Care Coordination Purposes, Michigan Department of Health and Human Services to CMH.

Documentation of Disclosure of Protected Health Information – The CCO, acting as the Privacy Officer is responsible to document disclosures of PHI. The information is documented in a database for tracking purposes. All records that have been disclosed are copied and maintained by the CCO for reference. This form may be completed as well along with the CCO copies of the disclosed records.

Request for Records Release – This form is completed by the person supported, guardian or employee to request copies of their records. The form is reviewed by the CCO for processing with the appropriate department. Other formats may be accepted from sources such as the Social Security Administration or attorneys.

PROCEDURE

1. Request for Access – The people we serve and or their legal guardian may request access to their records at any time. Any request made by an individual other than the person served or their legal guardian that does not fall under the category of Treatment, Payment and Health Care Operations must make their request for access to an individual's records in writing. If a satisfactory Release has not been provided with the request the CCO will request a Release of Confidential Information/ HIPAA Disclosure Authorization before allowing access to individual records.
2. Action on Request for Access – The CCO shall act on a request for access no later than thirty (30) calendar days after LADD's receipt of the request. Every effort will be made to provide the requested information in the timeframe given by the requestor. If the CCO is unable to act on the request within the applicable time required by the preceding paragraph the CCO may extend the time for the action by no more than thirty (30) calendar days, provided:

- a. Within the applicable time required by the preceding paragraph, the CCO shall provide the individual with a written statement of the reason (s) for the delay and the date by which LADD will complete its action on the request: and,
 - b. Only one such extension shall be permitted on a request for access.
3. Inform Individual on Action on Request – If the request is granted, in whole or in part, the CCO will provide the information requested. If the request is denied, in whole or in part, the CCO shall provide the individual with a written denial.
 4. Form and Format – The protected health information will be provided to the individual in the form or format requested by the individual, if it is readily producible in that form or format. If it is not readily producible in that form or format, it shall be provided in a readable hard copy form or such other form or format as agreed to by the CCO and the individual.
 5. Summary in Lieu of Access – The individual may be provided a summary of the protected health information requested, in lieu of providing access to the protected health information, or may be provided an explanation of the protected health information to which access has been provided if:
 - a. The individual agrees in advance to such a summary of explanation; and,
 - b. The individual agrees in advance to the fees imposed by LADD for such summary or explanation.
 6. Time and Manner of Access – Access shall be provided in a timely manner as stated in “Action on Request for Access,” including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy to the individual at the individual’s request. The CCO may discuss the scope, format and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
 7. Fees – If the individual requests a copy of the protected health information, or agrees to a summary or explanation of such information, LADD may impose charges as set forth under Fees for Accounting.
 8. Reviewable Grounds for Denial – LADD may deny an individual access, in any of the following circumstances; provided that the individual is given a right to have the denial reviewed as stated in “Review of Denial” below:
 - a. Endangerment- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
 - b. Reference to Another Person- The protected health information makes references to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
 - c. Personal Representative- The request for access is made by the individual’s personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
 - d. Other- Incident reports are peer review documents only and are not part of the clinical record and are not to be used as a substitute for clinical documentation. Data from incident reports shall only be used to look for methods and opportunities to improve services, determine and correct problems, identify potential violations of rights, and assist in trending for review of significant health risks to consumers and staff. An incident or peer review report generated pursuant to MCL 330.1143a does not constitute a summary report as intended by this section and shall not be maintained in the clinical record of a recipient. Further, Incident Reports are not public records, and are not subject to court subpoena
 9. Actions if Access is Denied – If an individual’s access to protected health information is denied, in whole or in part, LADD shall comply with the following:
 - a. Making Other Information Accessible- LADD shall, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information to which LADD had the ground to deny access.
 - b. Written Denial- CCO shall provide a written denial to the individual within the applicable time period. This denial shall contain:
 1. The basis for the denial.

2. If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights
 3. A description of how the individual may complain pursuant to L.A.D.D., Inc.'s complaint procedures or to the Secretary of Health and Human Resources, including the name or title, and the telephone number of the LADD contact person or office designated to receive complaints.
 4. If LADD does not maintain the protected health information that is the subject of the individual's request for access, and LADD knows where the requested information is maintained, a statement informing the individual where to direct the request for access.
10. Review of Denial – If access is denied on a ground permitted under “Reviewable Grounds,” the individual shall have the right to have the denial reviewed by a licensed health care professional who is designated by the CCO to act as a reviewing official and who did not participate in the original decision to deny.
- a. The individual's request for review shall be promptly referred to that designated reviewing official. The designated reviewing official shall then determine, within reasonable period of time, whether or not to deny the access requested based on the standards stated in “Reviewable Ground for Denial”.
 - b. The CCO shall then promptly provide written notice to the individual of the determination of the designated reviewing official and implement the designated reviewing official's determination.
11. Documentation – CCO shall maintain, or cause to be maintained, documentation of:
- a. The designated records that are subject to access by individuals; and,
 - b. The titles of the persons or offices responsible for receiving and processing request for access by individuals.

The documentation shall be maintained by LADD in written or electronic form for seven years after the date of its creation or the date when it was last in effect, whichever is later.

12. **EMPLOYEE ACCESS TO FILE** – Pursuant to Michigan law **BULLARD-PLAWECKI EMPLOYEE RIGHT TO KNOW ACT 397**, employees may review and request a copy of their personnel file. They may also file a response regarding the content of their personnel file. If an employee would like to review their personnel file, a written request must be submitted to the LADD Office.

The request for review should include the employee's name, dates of employment and the specific location at which the employee works or worked. Appointments will be scheduled during regular office hours, unless other arrangements are necessary. The examination of the file will be supervised, no contents of the file(s) are to be removed or destroyed.

If an employee requests a copy of the contents of their personnel file, LADD requires reimbursement at the current established rate. Copies will be made by LADD and given to the employee within 2 weeks of the request.

If there is a disagreement between LADD and the employee regarding the contents of the file, the employee may submit up to 5 pages (8.5x11) of written response. This response will be included when/if the personnel file is divulged to a third party at the employee's written request.

Employee files are kept at a minimum of seven years.



REQUEST FOR RELEASE OF RECORDS

I, _____, am requesting copies of records for _____ (Self or Ward), and would like them provided in the following format _____.

I understand that I must specify what records I would like to have copied, including type of record(s). Requests will be forwarded to the LADD Corporate Compliance Officer.

____ I would like to make an appointment to review my records with a member of LADD management. I will choose what copies I would like to obtain at that time.

____ I understand that I may be charged for each page copied at the rate of .25cents per page. Management will provide copies within 30 calendar days of the receipt of this signed release. Copies may be picked up and signed for at the LADD office, mailed (postage will apply), or emailed. Payment can be made through payroll deduction (if applicable), or in person at the LADD office.

Please mail my records to the following address:

____ Pick Up

____ Email to email address: _____

List of documents of which I would like copies: (Attach additional pages as needed.)

WE MAKE THE DIFFERENCE

Print Person's Name

Person's Signature

Date

Guardian's Signature

Date



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



RELEASE OF CONFIDENTIAL INFORMATION HIPAA DISCLOSURE

I _____ hereby authorize LADD to disclose and exchange
(My Name- Person Choosing Support Services)
confidential/protected information about me in accordance with the terms and provisions as described below.

- The name or other specific identification of the person(s) or class of persons, authorized to request, receive and disclose confidential information: LADD Employees
- The name or other specific identification of the person(s) or class of persons to whom the requested disclosure may be made:
 - Contract Agency and Employees: _____
 - Physicians and other Health Care Professionals _____
 - Hospitals/Emergency Medical Technicians _____
 - Pharmacy _____
 - Family Members _____
 - Friend's _____
 - School _____
 - Department of Health and Human Services _____
 - Law Enforcement, Emergency Personnel, Community members; in case of an Emergency _____
 - Other _____
- Specific description of the information to be used or disclosed:
 - Treatment Records and Information: _____
 - Medical/Health Records: _____
 - Information on current status of services provided: _____
- The information may be used or disclosed for each of the following purposes:
 - Safety and Protection
 - To provide coordination of care
 - To obtain benefits and services
 - To develop natural supports within their community
 - At the request of the individual
 - Other (please describe) _____
- Specify any restrictions regarding the release of information: _____

Personal statements about this disclosure of confidential/protected information:

- > I understand that I may withdraw my authorization at any time by notifying LADD at 300 Whitney Street Dowagiac, MI. 49047 in writing.
- > I understand also that such withdrawal of my authorization may not be effective to prevent disclosure of information previously authorized or to stop previous action that has been taken in reliance on this authorization.
- > I understand that some of my Protected Health Information is maintained in an electronic format.
- > I understand that, if the person or entity receiving this information is not covered by the Federal Privacy Regulations, such information may no longer be protected from further disclosure.
- > I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment.
- > I also understand that records concerning mental health services I receive are protected by the Michigan Mental Health Code.
- > My signature means that I have read this form and/or have had it read to me and explained in language I can understand. I know what information will be disclosed and give my voluntary consent to its release.
- > I understand disclosures of Protected Health Information will be made in accordance with the LADD Notice of Privacy Practices.
- > I understand that I am responsible to update this disclosure annually and this disclosure is in effect until the new one is received.

My Signature

Date

My Legal Guardian's Signature

Date

Management Signature

Date

(A copy of this fully completed and signed form needs to be retained by the person/legal guardian)



DOCUMENTATION OF DISCLOSURES INDIVIDUAL PROTECTED HEALTH INFORMATION

Person Supported Name and Address:

Case Number: _____

Date of Disclosure:

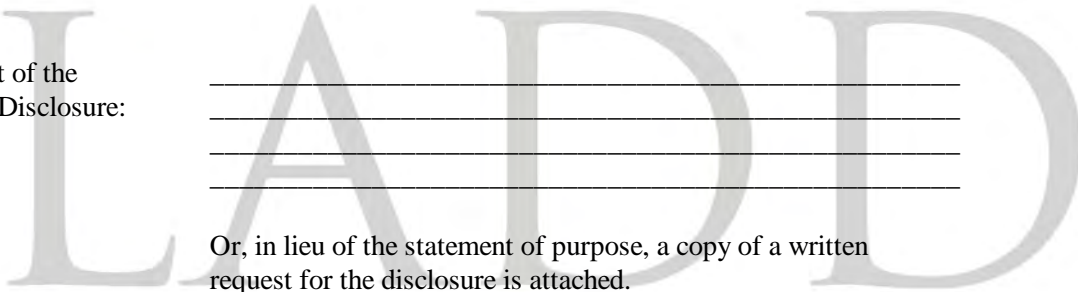
Name of Person/Entity
Receiving the Disclosure:

Address of Person/Entity
(If known):

Brief Description of the
Information Disclosed:

Brief Statement of the
Purpose of the Disclosure:

Or, in lieu of the statement of purpose, a copy of a written
request for the disclosure is attached.



WE MAKE THE DIFFERENCE

Corporate Compliance Officer

Date



BUSINESS ASSOCIATES

A business associate is an individual or company that works with LADD and:

- Creates, receives, maintains or transmits Protected Health Information with LADD.
- Not a part of the LADD workforce (on payroll as a regular employee).
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

An example of a business associate could be the company that maintains the LADD servers and computer system or electronic health record system.





BUSINESS ASSOCIATES POLICY

PURPOSE

To establish a policy for the identification and use of Business Associates to ensure Business Associates use confidential information only for the purposes LADD has contracted with them for, will safeguard confidential information from misuse and will comply with applicable HIPAA standards.

SCOPE

This policy applies to all LADD support services, employees and Business Associates.

POLICY

It is the policy of LADD to obtain satisfactory assurances from Business Associates that they will appropriately safeguard the PHI it receives or creates on behalf of LADD.

STANDARDS AND DEFINITIONS

Business Associate (BA) – A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to LADD. Functions performed by a BA may include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial activities.

Business Associates must not be excluded from any federal or state programs in order to be a Business Associate of LADD and must notify LADD immediately if they become excluded from participation in State or Federal health plans or have any sanctions imposed on them by Medicare or Medicaid. An employee of LADD is not a Business Associate.

Exceptions to Business Associate – A person or entity is NOT a BA if their function or service does not involve the use or disclosure of PHI and access to PHI would be incidental if at all. This may include general classifications such as janitorial, pest control, fire safety and other service related providers, fleet management and transportation and technology support. Additionally, a person or organization that acts merely as a conduit for PHI, such as the US Postal Service is not a BA.

Business Associate Contract (BAC) – An agreement entered into by LADD and a BA that describes the permitted and required uses of PHI by the BA, appropriate safeguards to prevent unauthorized use or disclosure of PHI. If LADD becomes aware of a violation of the contract; steps will be taken to correct the violation or terminate the contract.

Term of Business Associate Contract – The BAC shall be effective for the length of the relationship between the BA and LADD unless otherwise terminated under the provisions outlined in the BAC.

Corporate Compliance Officer – Responsible for overseeing the management of BA relationships and BACs which includes assessing existing and future vendor/business relationships to determine whether a BAC is needed.

PROCEDURE

1. The CCO in conjunction with the Compliance Committee will determine the need for a BAC.
2. The CCO will collect contact information for the BA.
3. The CCO will provide training and relevant policies to the pending BA.
4. The CCO will collect the BAC with the BA. In some circumstances, the BA will provide a copy of their BAC. Regardless of the format or where the BAC originates from the BAC will be signed by both parties and contain the required elements according to HIPAA standards.
5. The CCO will maintain the following information relative to the BA:
 - Name of the BA
 - Address and telephone number of the BA
 - Contact person and information for the BA
 - Date BAC executed
 - Date training completed
 - Type of work to be performed by BA.



LADD

WE MAKE THE DIFFERENCE



BUSINESS ASSOCIATE CONTRACT

THIS CONTRACT is made and entered into by and between Living Alternatives for the Developmentally Disabled, Inc. (hereinafter called "PROVIDER"), a covered entity, with its principal place of business located at 300 Whitney Street, Dowagiac, MI 49047

- AND -

_____ (hereinafter called "BUSINESS ASSOCIATE"),
a/an _____ corporation, with its principal place of business located
at _____

Recitals

- A. BUSINESS ASSOCIATE performs, or assists in the performance, of a function or activity or provides services of a type for PROVIDER that makes BUSINESS ASSOCIATE a "business associate" for purposes of the HIPAA privacy regulations.
- B. PROVIDER will disclose protected health information to BUSINESS ASSOCIATE in conjunction with the function, activity, or services performed or provided by BUSINESS ASSOCIATE.
- C. PROVIDER will disclose electronic protected health information to BUSINESS ASSOCIATE in conjunction with the function, activity, or services performed or provided by BUSINESS ASSOCIATE.
- D. PROVIDER and BUSINESS ASSOCIATE desire to enter into a contract as required by the HIPAA privacy and security regulations to provide satisfactory assurance to PROVIDER that BUSINESS ASSOCIATE will appropriately safeguard that protected health information.

Agreement

NOW THEREFORE, PROVIDER and BUSINESS ASSOCIATE agree as follows:

- (1) **Definitions.** All terms and phrases in this Contract shall have the same meanings as defined in 45 CFR §160 and §164, subparts A, C, D, and E. Without limiting the generality of the foregoing, as used in this Contract, the following terms shall have the following meanings:
 - (a) "HIPAA privacy regulations" shall mean the regulations at 45 CFR §160 and §164, subparts A and E.
 - (b) "HIPAA security regulations" shall mean the regulations at 45 CFR §160 and 164, subpart C.
 - (c) "HIPAA Breach Notification Rule" shall mean the regulations at 45CFR §164, subpart D.
 - (d) "HIPAA Rules" shall mean the HIPAA privacy regulations, the HIPAA security regulations, the HIPAA Breach Notification Rule, and the HIPAA enforcement rule at 45 CFR §160, subpart C.
 - (e) "Secretary" shall mean the Secretary of the United States Department of Health and Human Services ("HHS") or any other officer or employee of HHS to whom the authority involved has been delegated.
 - (f) "Protected health information" shall mean individually identifiable health information regardless of whether it is maintained in electronic or non-electronic form.

- (g) “Electronic protected health information” shall mean individually identifiable health information that is transmitted by or maintained in electronic media. It includes devices in computers and any removable/transportable digital memory medium. Transmission media include the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and physical movement of removable/transportable media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
- (h) “Security incident” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(2) **Restriction on Use and Disclosure of Protected Health Information.** Except as permitted or required by this Contract or as required by law, BUSINESS ASSOCIATE shall not use, de-identify, or further disclose any protected health information disclosed or otherwise made available to it by PROVIDER.

(3) **Authorized Uses and Disclosures.** Except as otherwise limited in this Contract, BUSINESS ASSOCIATE is hereby authorized to use and disclose protected health information for the following purposes:

(a) **Generally -** BUSINESS ASSOCIATE may use or disclose protected health information on behalf of, or to provide services to, PROVIDER for the following purposes, if such use or disclosure of protected health information would not violate the HIPAA privacy regulations if done by PROVIDER or the minimum necessary policies and procedures of PROVIDER.

(b) **Management and Administration -** BUSINESS ASSOCIATE may use and disclose protected health information for the proper management and administration of BUSINESS ASSOCIATE or to carry out the legal responsibilities of BUSINESS ASSOCIATE, provided:

(1) The disclosure is required by law; or,

(2) BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person and the person will immediately notify the BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) **Date Aggregation Services.** BUSINESS ASSOCIATE may use and disclose protected health information to provide data aggregation services relating to the health care operations of PROVIDER.

(d) **Violations of Law.** BUSINESS ASSOCIATE may use protected health information to report violations of law to appropriate Federal and State authorities, consistent with

(4) **BUSINESS ASSOCIATE’S Obligations.**

(a) **Representation and Acknowledgment.** BUSINESS ASSOCIATE represents that it has complied and will comply with the requirements of the HIPAA Rules applicable to it and acknowledges that it is aware that it is subject to the tiered civil and criminal penalties of section 1176 and 1177 of the Social Security Act.

(b) **Safeguards.** BUSINESS ASSOCIATE shall use appropriate safeguards, and comply, where applicable, with the HIPAA security regulations with respect to electronic protected health

information, to prevent use or disclosure of protected health information other than as permitted or required by this Contract or as required by law.

- (c) **Security of Electronic Protected Health Information.** BUSINESS ASSOCIATE shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of PROVIDER.
- (d) **Reporting.** BUSINESS ASSOCIATE shall report to PROVIDER any use or disclosure of protected health information not permitted by this Contract of which it becomes aware, including breaches of unsecured protected health information as required by the HIPAA Breach Notification Rule. Furthermore, BUSINESS ASSOCIATE shall report to PROVIDER any security incident of which it becomes aware. This report shall be given to PROVIDER as soon as possible after BUSINESS ASSOCIATE discovers the impermissible use or disclosure but not more than 5 days after the discovery.
- (e) **Subcontractors.** BUSINESS ASSOCIATE shall ensure that any subcontractors, that create or receive protected health information on behalf of BUSINESS ASSOCIATE agree to the same restrictions and conditions that apply to BUSINESS ASSOCIATE with respect to such information.
- (f) **Providing Electronic Protected Health Information to Agents or Subcontractors.** BUSINESS ASSOCIATE shall ensure that any agent, including a subcontractor, to whom it provides electronic protected health information, agrees to implement reasonable and appropriate safeguards to protect the electronic protected health information.
- (g) **Individual's Access to Information.** BUSINESS ASSOCIATE shall make available and permit access to protected health information about an individual by that individual in accordance with 45 CFR §164.524.
- (h) **Amendment of Protected Health Information.** BUSINESS ASSOCIATE shall make available to PROVIDER protected health information for amendment and incorporate any amendments to protected health information in accordance with 45 CFR §164.526.
- (i) **Accounting of Disclosures.** BUSINESS ASSOCIATE shall document such disclosures of protected health information and information related to such disclosures as would be required for PROVIDER to respond to a request by an individual for an accounting of disclosures of protected health information in accordance with 42 CFR. §164.528.

BUSINESS ASSOCIATE shall make available the information required to provide an accounting of disclosures in accordance with 42 CFR. §164.528. Such information shall be given to PROVIDER by BUSINESS ASSOCIATE within 5 days after PROVIDER notifies BUSINESS ASSOCIATE of PROVIDER's need for the information.
- (j) **Comply with PROVIDER's Obligations.** To the extent BUSINESS ASSOCIATE is to carry out PROVIDER's obligations under the HIPAA privacy regulations, BUSINESS ASSOCIATE shall comply with the requirements of the HIPAA privacy regulations that apply to PROVIDER in the performance of such obligations.
- (k) **Practices, Books and Records.** BUSINESS ASSOCIATE shall make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by BUSINESS ASSOCIATE on behalf of PROVIDER, to the Secretary for the purpose of determining PROVIDER's compliance with the HIPAA privacy regulations.

- (l) **Mitigation.** BUSINESS ASSOCIATE shall mitigate, to the extent practicable, any harmful effect that is known to BUSINESS ASSOCIATE or to PROVIDER of a use or disclosure of protected health information in violation of BUSINESS ASSOCIATE's policies and procedures, this Contract, or the HIPAA privacy or security regulations.

(5) **PROVIDER's Obligations.**

(a) **Provisions for PROVIDER to Inform BUSINESS ASSOCIATE of Privacy Practices and Restrictions.**

- (1) PROVIDER shall notify BUSINESS ASSOCIATE of any limitations(s) in its Notice of Privacy Practices of PROVIDER in accordance with 45 CFR §164.520, to the extent that such limitation may affect BUSINESS ASSOCIATE's use or disclosure of protected health information.
- (2) PROVIDER shall notify BUSINESS ASSOCIATE of any changes in, or revocation of, permission by an individual to use or disclose protected health information, to the extent that such changes may affect BUSINESS ASSOCIATE's use or disclosure of protected health information.
- (3) PROVIDER shall notify BUSINESS ASSOCIATE of any restriction to the use or disclosure of protected health information that PROVIDER has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect BUSINESS ASSOCIATE's use or disclosure of protected health information.

(b) **Permissible Requests by PROVIDER.**

PROVIDER shall not request BUSINESS ASSOCIATE to use or disclose protected health information in any manner that would not be permissible under the HIPAA privacy regulations if done by PROVIDER.

(6) **Breach Notification.**

- (a) **Notice to PROVIDER.** In the event of its discovery of a breach of unsecured protected health information disclosed or made available to it by PROVIDER, BUSINESS ASSOCIATE shall provide notification of such breach to PROVIDER as required by the HIPAA Breach Notification Rule. Provided, however, notwithstanding anything in that Rule to the contrary or in paragraph (16) of this Contract, such notice shall be given to PROVIDER by BUSINESS ASSOCIATE as soon as possible after BUSINESS ASSOCIATE's discovery of the breach, but in no case more than 5 calendar days after its discovery of the breach.
- (b) **Notice of Breach to Affected Individuals; Costs.** Whether or not notification of the breach shall be given to affected individuals and, if so, the method by which the notification shall be given shall be determined by PROVIDER, in its sole discretion. If required by PROVIDER in its sole discretion, BUSINESS ASSOCIATE shall give any such notice(s) at such times and in such manner as determined by PROVIDER. In all cases, BUSINESS ASSOCIATE shall pay to PROVIDER the costs incurred by PROVIDER due to the breach.
- (c) **Proof of Encryption.** In the event of a breach of secured protected health information, BUSINESS ASSOCIATE shall notify PROVIDER of the breach as stated in subparagraph (6)(a), above, and, within 5 calendar days after giving such notice to PROVIDER, provide proof satisfactory to PROVIDER that such protected health information was not unsecured protected health information.

(7) **Term and Termination.**

(a) **Generally.** This Contract shall be effective when executed on behalf of both of the parties hereto and shall terminate when all of the protected health information provided by PROVIDER to BUSINESS ASSOCIATE, or created or received by BUSINESS ASSOCIATE on behalf of PROVIDER, is destroyed or returned to PROVIDER, or, if it is not feasible to return or destroy protected health information, protections are extended to such information, in accordance with the termination provisions in this Paragraph (7).

(b) **Mutual Agreement.** This Contract may be terminated by mutual written agreement of the parties.

(c) **Termination for Cause.** Upon PROVIDER's knowledge of a material breach of this Contract by BUSINESS ASSOCIATE, PROVIDER shall either:

- (1) Provide an opportunity for BUSINESS ASSOCIATE to cure the breach or end the violation and terminate this Contract if BUSINESS ASSOCIATE does not cure the breach or end the violation within the time specified by PROVIDER;
- (2) Immediately terminate this Contract if BUSINESS ASSOCIATE has breached a material term of this Contract and cure is not possible.

(d) **Effect of Termination.**

- (1) Except as provided in paragraph (2), below, upon termination of this Contract, for any reason, BUSINESS ASSOCIATE shall return or destroy all protected health information received from PROVIDER, or created or received by BUSINESS ASSOCIATE on behalf of PROVIDER that BUSINESS ASSOCIATE maintains in any form. This provision also shall apply to protected health information that is in the possession of subcontractors of BUSINESS ASSOCIATE. BUSINESS ASSOCIATE shall retain no copies of the protected health information.
- (2) In the event that BUSINESS ASSOCIATE determines that returning or destroying the protected health information is not feasible, BUSINESS ASSOCIATE shall provide to PROVIDER notification of the conditions that make return or destruction not feasible. BUSINESS ASSOCIATE shall extend the protections of this Contract to such protected health information and limit further uses and disclosures of such protected health information to those purposes that make the return or destruction not feasible, for so long as BUSINESS ASSOCIATE maintains such protected health information.

(8) **Injunction.** Notwithstanding any other rights or remedies provided for in this Contract, PROVIDER retains all rights to injunctive relief to prevent or stop the unauthorized use or disclosure of protected health information by BUSINESS ASSOCIATE, or any agent, subcontractor or other third party that received protected health information from BUSINESS ASSOCIATE.

(9) **Indemnification.** BUSINESS ASSOCIATE shall indemnify and hold PROVIDER harmless from and against any and all loss, cost, damage, or expense, including reasonable attorneys' fees, that arise out of: any breach by BUSINESS ASSOCIATE of this Contract, the HIPAA privacy regulations; the HIPAA security regulations, or the HIPAA Breach Notification Rule, or, the need for PROVIDER to enforce any provision of this Contract.

(10) **Subpoena.** In the event BUSINESS ASSOCIATE receives a subpoena for any protected health

information in BUSINESS ASSOCIATE's possession, BUSINESS ASSOCIATE shall immediately notify PROVIDER of the subpoena and deliver a copy of the subpoena to PROVIDER. BUSINESS ASSOCIATE shall respond to the subpoena only in accordance with the HIPAA privacy regulations.

(11) **Notices.** Any notices required or permitted to be given under this Contract shall be in writing and shall be personally delivered or sent by certified or registered mail, first class postage prepaid, return receipt requested, or by prepaid overnight delivery service such that proof of delivery will be obtained, and shall be addressed as set forth below or to such other address as may be specified in a prior written notice to the other party:

(a) If to PROVIDER:
300 Whitney,
Dowagiac, MI 49047

(b) If to BUSINESS ASSOCIATE

Such notice shall be deemed to be given on the date it is deposited in the mail as stated above, on the date it is given to the overnight delivery service, or the date it is given personally to the party to whom it is directed. A notice shall be deemed to have been given personally to a party if it is handed to the representative of the party to whom the notice must be addressed or if left at his or her office located at the street address to which a notice would be mailed.

- (12) **Amendment.** This Contract may not be changed, modified, or amended except by a written agreement executed on behalf of each of the parties.
- (13) **No Waiver.** No waiver of one or more of the provisions of this Contract or the failure to enforce any provision of this Contract by either party shall be construed as a waiver of any subsequent breach of this Contract, nor a waiver of the right at any time thereafter to require strict compliance with all of its terms.
- (14) **Entire Agreement.** This Contract sets forth the entire agreement and understanding between the parties as to the matters contained in it, and supersedes all prior discussions, agreements, and understandings of every kind and nature between them.
- (15) **Headings.** The headings placed before the various paragraphs and subparagraphs of this Contract are inserted for ease of reference only, do not constitute a part of this Contract, and shall not be used in any way whatsoever in the construction or interpretation of this Contract.
- (16) **Interpretation.** Any ambiguity in this Contract shall be resolved to permit Covered Entity to comply with the HIPAA Privacy Rule, 45 CFR § 164.500 *et seq.*, the HIPAA Security Rule, 45 CFR § 164.302 *et seq.*, and the HIPAA Breach Notification Rule, 45 CFR § 164.400 *et seq.*, as each may be amended from time to time.
- (17) **Governing Law.** This Contract shall be construed and enforced in accordance with, and governed by, the laws of the State of Michigan.

IN WITNESS WHEREOF, the parties hereto have caused this Contract to be executed by their duly authorized representatives on the dates set forth below.

Attest:

PROVIDER

(signature)

By: _____
(print)

Title: _____

Attest:

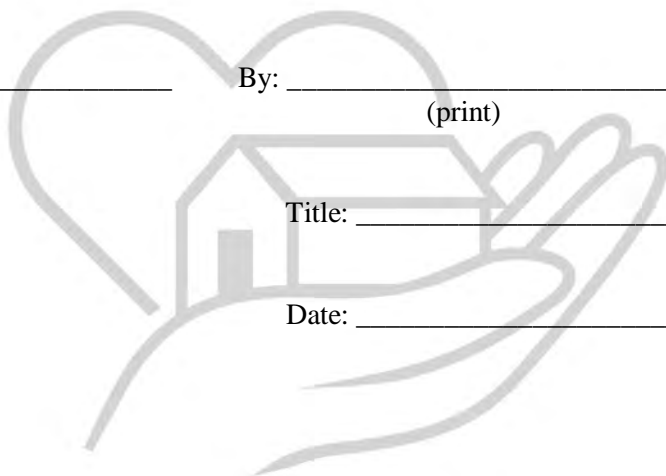
BUSINESS ASSOCIATE

(signature)

By: _____
(print)

Title: _____

Date: _____



LADD

WE MAKE THE DIFFERENCE



BREACH RESPONSE

When personal and confidential information is released to a person who is not authorized to have that information. Or if that information is no longer within the oversight and protection of LADD systems it is critical to immediately report the incident as soon as it is discovered to a member of Management.

Management will take the report to the Corporate Compliance Officer, who acts as the Privacy Officer at LADD so the incident can be addressed. Not every incident will meet the definition of a breach, requiring a structured response, so until it does it should be viewed simply as a **security incident**. Only after the procedures in this section are followed and a proper investigation and analysis takes place can appropriate corrective action.



LADD

WE MAKE THE DIFFERENCE



HIPAA BREACH RESPONSE POLICY

PURPOSE

To establish a policy for the identification of and response to suspected or known breach incidents. Mitigate harmful effects of breach incidents. Document all breach incidents and their outcomes.

SCOPE

This policy applies to all LADD support services, employees, business associates and persons supported.

POLICY

It is the policy of LADD to have established procedures for the reporting, identification, investigation and mitigation of all breaches of unsecured protected health information.

STANDARDS AND DEFINITIONS

Unsecured Protected Health Information (uPHI) - uPHI is Protected Health Information (PHI) that has **NOT** been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS as follows:

- Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached.
- The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
 - Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. **Redaction**, or removal of sensitive information is specifically excluded as a means of data destruction.
 - Electronic media have been cleared, purged, or destroyed such that the PHI cannot be retrieved.

Breach - An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless LADD or a Business Associate (BA) demonstrates there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of PHI involved, including types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

Exceptions to Breach Definition - There are three exceptions to the definition of “breach.”

- Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of LADD or BA, if such acquisition, access, or use was made in good faith and within the scope of authority.
- Inadvertent disclosure of PHI by a person authorized to access PHI employed with LADD or BA to another person authorized to access PHI within LADD or BA, or organized health care arrangement in which LADD participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- LADD or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

HIPAA Breach Assessment Tool - Document completed as part of the investigation process to determine if a breach has occurred.

Notification – LADD is required to and will notify people supported, and if applicable their legal guardian and the contract agency if it is determined there has been a breach of PHI. LADD will take steps to mitigate risks identified with the breach which could include monitoring by an identity theft and fraud detection monitoring service LADD will notify as required any person and legal guardian if applicable, as well as the contract agency if applicable if it is determined there has been a breach of PHI.

LADD will notify affected individuals following the discovery of a breach of uPHI as follows;

- Provide individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
- If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- Will include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.
- Will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include;
 - A brief description of the breach.
 - A description of the types of information that were involved in the breach.
 - The steps affected individuals should take to protect themselves from potential harm.
 - A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches.
 - Contact information regarding questions.
- LADD will maintain proof demonstrating that all required notifications have been provided or that a use or disclosure of uPHI did not constitute a breach.

Breach Notification Requirements –

If a breach of uPHI affects **500 or more** individuals, LADD must notify the Secretary of the Office of Civil Rights of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. A separate notice must be completed for each breach incident. LADD must submit the notice electronically to the Office for Civil Rights.

If a breach of uPHI affects **fewer** than 500 individuals, LADD must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered and may notify sooner at LADD's discretion. A separate notice must be completed for each breach incident. Notice must be submitted electronically to the Office for Civil Rights.

PROCEDURE

1. Upon discovery of a suspected release of uPHI the person making the discovery will immediately report the incident to the Corporate Compliance Officer (CCO).
2. The CCO will begin an investigation and complete the HIPAA Breach Assessment Worksheet that includes:
 - a. Date
 - b. Person reporting
 - c. Description of the incident

- d. Develop list of questions to help determine how the breach occurred looking for possible risk areas in the company.
 - e. Develop a list of individuals to be interviewed
 - f. Identify gaps, additional risks
 - g. Identify additional, supporting pieces of information
 - h. Develop recommendations and contingencies
3. The CCO will report findings to the Executive Director or their designee.
4. The Executive Director or their designee may consult with Corporate Counsel at this point to determine the correct legal approach. The CCO will be included as necessary in order to complete the recommended action.
5. CCO will complete notifications per the notification section in Standards and Definitions of this Policy.
6. CCO will coordinate with the appropriate LADD personnel to ensure the following has been completed:
 - a. Ongoing follow up that was included in the notification letter has been completed with individuals affected by the breach.
 - b. Implement system changes to reduce/eliminate the possibility of future breaches
 - c. Train LADD employees of the system change.
7. The CCO will maintain all documentation relative to the incident.



LADD

WE MAKE THE DIFFERENCE





HIPAA BREACH ASSESSMENT WORKSHEET

Date:

Person Reporting:

<u>DETERMINATION FACTOR</u>	<u>RESULTS/FINDINGS</u>
People Involved- Name and Position	
DESCRIPTION OF INCIDENT	
WAS THE PHI INVOLVED IN THE INCIDENT UNSECURED? Unsecured PHI is defined as “PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance.” The guidance specifies the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. Encryption and destruction are identified as the two technologies and methodologies for meeting the requirements.	
1. DESCRIBE THE TYPE OF INFORMATION WHAT ARE THE TYPES OF IDENTIFIERS CAN THE INFORMATION BE RE-IDENTIFIED	

<u>DETERMINATION FACTOR</u>	<u>RESULTS/FINDINGS</u>
2. WHO (NAME OR POSITION) GAINED UNAUTHORIZED USE OF INFORMATION OR DISCLOSURE OF INFORMATION	
3. WAS THE INFORMATION ACQUIRED OR VIEWED	
4. STEPS TAKEN TO MITIGATE HARM PHI RETURNED AND/OR DESTROYED	
DO ANY OF THE FOLLOWING EXCEPTIONS APPLY <ul style="list-style-type: none"> • Was PHI unintentionally accessed by a LADD Inc. or BA employee acting within the scope of their authority? • Was PHI inadvertently disclosed by an authorized LADD Inc. or BA employee to another LADD Inc. or BA employee in which LADD Inc. participates in business with? • LADD Inc. or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information? 	

<u>DETERMINATION FACTOR</u>	<u>RESULTS/FINDINGS</u>
<p>DID A VIOLATION OF THE HIPAA PRIVACY RULE OCCUR</p> <p>HAS THERE BEEN A BREACH OF UNSECURED PHI REQUIRING REPORTING UNDER THE BREACH NOTIFICATION RULES? (Is there a low probability PHI was compromised)</p>	
<p>FINDINGS/ACTION TO BE TAKEN</p>	

Additional Information that may be needed to investigate the breach

Are there other individuals involved who may have knowledge of the breach?

Questions that may assist to identify the root cause of the breach?

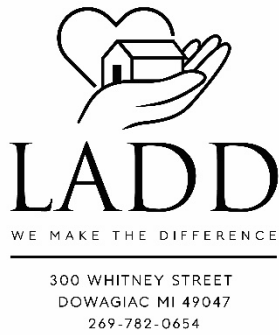
Questions that may assist to identify possible risk to the company?

Is there any other supporting information needed in assessing the breach?

Are there any recommendations to reduce or eliminate future breaches?

LAADD

WE MAKE THE DIFFERENCE



(Date)

(Person's Name)

(Person's Address)

Dear (Person),

We are sending this letter to you as part of LADD Inc.'s commitment to the privacy of every individual we support. We take person supported privacy very seriously, and it is important to us that you are made fully aware of a potential privacy issue. We have learned that your personal information, including name, address, (list additional as needed), may have been compromised. On (specify date of incident discovered), it was discovered that (give details of the incident). We reported the incident to the police because theft may have been involved (if applicable). However, we have not received any indication that the information has been accessed or used by an unauthorized individual.

We are aware of how important your personal information is to you and have a few options for you to choose from in order to take steps to protect yourself. If you choose, as a measure of added security, we are offering one year of credit monitoring and reporting services at no cost to you. This service is performed through (name of service), an organization that watches for and reports to you unusual credit activity, such as creating new accounts in your name. (name of service) will also request that the three credit bureaus place a "Fraud Alert" on your credit report. If you would like to receive this service, please respond yes by (give deadline date).

We understand that this may be an inconvenience to you. We sincerely apologize and regret this situation has occurred. LADD Inc. is committed to providing quality care, including protecting your personal information, and we want to assure you that we have policies, procedures and dedicated staff to protect your privacy.

If you want to take advantage of the free credit monitoring service, or if you have any questions, please contact me at 269-782-0654.

Sincerely,

Ted Coffeen



INFORMATION AND TECHNOLOGY MANAGEMENT SYSTEMS

LADD utilizes several systems to make sure that personal and confidential information is protected and accessible. In order to achieve this a comprehensive approach to organizing and securing information and technology systems is divided into three basic categories:

- Administrative – training, auditing, reporting
- Physical – locked doors, screen protectors
- Technical – login passwords, wireless passwords

The information in this section is related to these categories.



LADD

WE MAKE THE DIFFERENCE



INFORMATION ACCESS POLICY

PURPOSE

To establish a policy that identifies the steps taken to maintain an adequate level of security to protect PHI, LADD data and information systems from unauthorized access.

SCOPE

This policy applies to all LADD support services, employees and business associates.

POLICY

It is the policy of LADD to have established procedures to insure only secure, approved access to PHI, data and information systems is allowed; that correct levels of access are monitored and reporting mechanisms are in place so corrective action is taken immediately.

STANDARDS AND DEFINITIONS

Level of Access – Notes the level of access each Asset User is given based on job responsibilities and need to know.

Remote Desktop Drives	Staff	Assistant Manager	Manager	Supervisor	Support Supervisor (By Dept)	Regional Director	Department Director	Executive Director
Website Employee Section	X	X	X	X	X	X	X	X
All Staff (P)	X	X	X	X	X	X	X	X
General (K)	X	X	X	X	X	X	X	X
Committee (E)	X	X	X	X	X	X	X	X
All Managers (O)			X	X	X	X	X	X
Manager (R)			X	X	X	X	X	X
Supervisor (J)				X		X	X	X
Management Coverage (L)			X	X		X	X	X
Corporate Quality (I)				X	X	X	X	X
Administration (G)						X	X	X
Human Resources (W)					X		X	X
Finance (Z)					X		X	X
Quality Assurance (Y)					X		X	X
LADD IT (X)					X		X	X
QI and Training (Q)					X		X	X
FOI (V)								X
Executive (K)								X

Applications	HR Dept	IT Dept	Compliance Dept	QA Dept	Training Dept	Services Dept
AOD	X				X	X
File Hold	X	X				
Therap		X	X	X		X

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. Supervisors are responsible for ensuring Asset Users know their responsibilities and are immediately reporting theft, loss or damage to the asset. In addition, Asset Users must:

- Routinely verify the accuracy of email addresses used to send emails
- Use **ladd secure** to secure all emails that contain PHI and are going outside of the closed LADD remote desktop system to insure proper encryption takes place.
- Will maintain login and password per LADD standards.
- All computers used by Authorized Users that are connected to the LADD Information Technology Network, must continually execute approved Virus-scanning Software per the LADD IT Department.

Asset User Authentication – Each Asset User will, at all times utilize their unique user name, password and any additional authentication measures to secure access to all IT assets and verify their identity. User name and password is never to be shared or given out. Asset Users are responsible for all action taken under their sign on. All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. All users must be required to change their passwords at least once every 60 days using the following criteria:

Follow these guidelines when creating a password:

- The password must be 7 to 32 characters long.
- The password must contain a mix of letters, numbers, and/or special characters. Passwords containing only letters or only numbers are not accepted.
- The password is case-sensitive.
- Single quotes, double quotes, ampersands (' " &), and spaces are not allowed.
- Successive passwords should not follow a pattern.
- Do not post or share your password or send your password to others by email.

Do not communicate or give user names or passwords to others or allow the use of a user name or password by others at any time. **Email Activities** – Special precaution is to be taken whenever using email. The following guidelines must be followed:

- Always secure PHI by encrypting email using **ladd secure** in the subject line of the email,
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email SPAM).
- Any form of harassment via email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Creating or forwarding Chain email, Phishing, or other scams of any type.
- Solicitation of email for any other email address, other than that of the Authorized User's own account, with the intent to harass or to collect replies is prohibited.

- Creating or forwarding Chain email, Phishing, or other scams of any type is prohibited.

Workstation Access Control – Each IT asset that has the ability to be set with an auto log off, time out after no activity and password enabling will be set by the IT Dept. prior to being put into service. All workstations must utilize the installed access controls. Active workstations are not to be left unattended for extended periods and should be logged off when not in use. Automatic Logoff. If an information system has an automatic logoff capability, then the feature will be enabled to terminate an electronic session after a predetermined time of inactivity.

Minimum Necessary – PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose, responsibility or function of the job. Based on the “Need to Know”.

Disclosure Notice – a notice warning Asset Users they must only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.

PROCEDURE

1. All employees will be given basic access at the staff level as part of the orientation process.
2. For Management level or higher, after completion of the IT Dept. orientation the IT Director will submit a request for access, via email to NSO following the level of access grid above.
3. If there are requests for additional access the IT Director will contact the CCO for approval of the appropriate access level.
4. The CCO will verify the correct level of access for the employee with their Supervisor or HR Dept. and respond to the IT Dept. email with approval and the level of access to be given.
5. If an employee becomes aware of access levels that are not in line with the minimum necessary, they will notify the CCO immediately. The CCO will in turn work with the IT Director to correct access immediately.
6. The IT Dept. will periodically audit and complete regular maintenance to email addresses and email groups.
7. If an employee is suspended or separated their login access will be discontinued as part of the Separation Notice process.
8. If a member of management is suspended or separated their login access will be discontinued immediately as part of the Discharge Management Checklist.
9. The IT Dept. will periodically audit for correct access levels to PHI, LADD data and information systems.
10. The IT Dept. will maintain website security software per the Technology Plan and periodically audit for unauthorized access.

VIOLATIONS

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



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 be 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.



WORKSTATION ACCESS AND FACILITY SECURITY POLICY

PURPOSE

To establish a policy that provides guidance for workstation security that includes the types and locations of workstations, the approved functions of those workstations and the measures to be used to protect access to information at those workstations.

SCOPE

This policy applies to all LADD support services, and employees.

POLICY

It is the policy of LADD to have established procedures to ensure the confidentiality and availability of PHI to authorized users.

STANDARDS AND DEFINITIONS

Types of Workstations

Location	Workstation Description and Permissible Uses	Access
Remote Workstation	A workstation at a personal residence consisting of either a desktop or laptop and multi-function device. To be used to carry out job responsibilities and support stakeholders.	Director Department Director Regional Director Office Support Staff
Mobile Workstation	A workstation that can be moved and consists of either a laptop or notebook. To be used to carry out the functions of job responsibilities and support stakeholders.	Director Department Director Regional Director Supervisor
Central Office Workstation	A workstation at designated office space with support staff providing administrative support for stakeholders. These workstations consist of desktops, printers, scanners, fax and copier	Director Department Director Regional Director Supervisor Office Support Staff
Program Workstation	A workstation at a LADD operated location such as a licensed program. The workstation is in space designed as office space and consists of desktops, printer, scanner, fax and copier to be used to carry out the functions of the location and support stakeholders.	Supervisor Manager Assistant Manager
Service Site Workstation-Management	A workstation located at a person supported residence. The workstation may be in a designated office space or may be in an area of the home deemed appropriate by the person. The equipment may include a desktop, printer, scanner, fax and copier to be used to carry out the functions of the location and support stakeholders.	Supervisor Manager Assistant Manager
Service Site Workstation-Staff	A workstation located at a person supported residence. The workstation is in an area of the home deemed appropriate by the person. The equipment may include a desktop and printer to be used by staff for documentation. This may include an I pad or tablet to be used in the community for documentation.	Supervisor Manager Assistance Staff (PCT)

Physical Safeguards – Action taken to prevent unauthorized access to PHI and protect buildings and equipment from natural disasters and unauthorized intrusion. May consist of locks, keys, key fobs, screen protectors, strategic placement of screens, alarm systems,

Technical Safeguards – Technology used to secure against unauthorized access to PHI and protect buildings and equipment from natural disasters and unauthorized intrusion. May consist of individualized User ID, password and secondary authentication, , use of software, prohibitions against use devices in conjunction with LADD IT Asset.

*****The following measures must be implemented where applicable*****

- Workstations will be located in secure areas with locked doors or in locked cabinets with keys available to authorized staff only.
- Use of a HIPAA Visitor Log to maintain a list of people who have been in and out of the locations.
 - Steps employees take to validate a person's identity
 - A requirement that all visitors must sign in, including time of arrival and purpose of visit i.e. repair refrigerator, visit family
 - What employees are to do in the event of unauthorized entry or a visitor is not in an area that coincides with the stated purpose of their visit
 - Visitors includes maintenance and repair workers, deliveries and sales people so that all entry to the facility is noted.
 - Visitors may be escorted to the location that coincides with their stated purpose of visit
- Use of AOD to maintain a schedule of employees who are working at locations.
- Use of Emergency Guidelines to minimize the impact of natural or manmade disasters.
- Asset Users will position computer screens away from traffic areas or common areas accessed by visitors.
- Asset Users will not connect removable storage devices to any workstation, this is prohibited
- Asset Users will not save confidential information on workstations unless it is appropriately secured against theft or loss and consult with the IT Dept. or CCO regarding appropriate steps to secure.
- Confidential information, based on the concept of minimum necessary should be saved in folders with access limited to those individuals authorized to access the information.
- Asset Users must logoff or lock their workstations when not in use.
- When appropriate, Asset Users should use a privacy screen to prevent unauthorized people from viewing information on their workstation screen.
- Asset Users must never install software on LADD IT Asset.
- A user ID and password must be required to use all workstations.
- All special access rooms that contain sensitive equipment or information i.e. workstations, file rooms, offices, fax/copy rooms will be locked with appropriate signage prohibiting unauthorized access.
- All LADD faxes will utilize a standardized, approved organizational fax cover and the original faxed information and cover are maintained when part of the person supported record to guard against altering faxed information.
- All unwanted and confidential documents will either be immediately shredded or placed in a bin that is secured against unauthorized access until the documents can be disposed of.
- The chain of custody for keys to secure areas will be monitored at all times and in the event, keys are lost it will be reported to the immediate Supervisor.
- In the event of an unhappy ex-employee who has made threats against another employee, person supported/family or the facility it will be reported to the immediate Supervisor, Human Resource Director and CCO.
- In the event an outside source has made threats against another employee, person supported/family or the facility it will be reported to the immediate Supervisor, Human Resource Director and CCO.

VIOLATIONS

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



RECORD RETENTION AND ASSET MANAGEMENT POLICY

PURPOSE

The purpose of the Record Retention and Asset Management Policy is to establish an efficient companywide record management system for maintaining, identifying, retrieving, preserving and destroying records. Additionally, to ensure that records are adequately protected, preserved and that records that are no longer needed or of no value are destroyed at the appropriate time, and manner in compliance with all applicable local, state, and federal laws and regulations.

SCOPE

This policy applies to all LADD employees and Business Associates relative to records generated in the course of LADD operations, including original documents, reproductions and electronic versions.

POLICY

It is the policy of LADD to establish procedures that adequately protect, maintain and destroy records that have been generated in the course of business and service operations; and provide a mechanism for reporting and resolving violations of this policy.

STANDARDS AND DEFINITIONS

Corporate Compliance Officer (CCO) – The CCO is responsible for the administration of this policy including directing subpoenas, requests for records, audits, external investigation, storage and disposal of records and assets and resolving complaints or reports of policy violation.

Protected Health Information (PHI) – Individually identifiable health information that is transmitted by electronic media, maintained in electronic form or that is maintained or transmitted in any other form. Info is PHI if it relates to physical/mental health or condition of an individual, provision of health care or payment for provision of health care.

Security of PHI – All locations, departments and business associates must protect PHI in accordance with relevant laws and the LADD HIPAA Privacy and Security Plan.

Suspension of Record Disposal in Event of Litigation or Claims – In the event LADD is served with any subpoena or request for record, or any employee becomes aware of a governmental investigation or audit concerning LADD or the commencement of any litigation against or concerning LADD, such employee shall inform the CCO and any further disposal of documents shall be suspended until such time the CCO, with the advice of counsel, determines otherwise

Physical Storage Facilities – Approved storage location that ensures the preservation of records in their original condition in a method that promotes efficient retrieval. Storage facilities must be secured against unauthorized access, maintain access logs and where applicable protect against pest infestation, fire, smoke, or water damage.

Correspondence, Internal Memoranda and Email – Most correspondence, internal memoranda and email should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records supporting a particular project be kept with the project and take on the retention time of that particular project file.

- **No Prescribed Period**— Correspondence, memoranda and email that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:
 - a. Those pertaining to routine matters and having no significant, lasting consequences should be discarded *within two years*. Some examples include:
 1. Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
 2. Form letters that require no follow-up.
 3. Letters of general inquiry and replies that complete a cycle of correspondence
 4. Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
 - b. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.
- **Email** – Not all email needs to be retained and depends on the subject matter.
 - a. E-mail—from internal or external sources—may be deleted after 12 months.
 - b. Employees will strive to keep all but an insignificant minority of their e-mail related to business issues.
 - c. Any e-mail employees deem vital to the performance of their job should be copied to the staff’s H: drive folder, and printed and stored in the employee’s workspace.

Destruction of Records – Expired Records must be destroyed in the following manner at the direction of the CCO.

- Hardcopy Records must be shredded in a manner that renders them unreadable and that would prevent them from being reconstructed. Security of the Expired Records must be maintained until proper destruction is actually performed.
- Electronic Records will be destroyed according to current and available technology in conjunction with the LADD IT Director. Methods may include disintegration, incineration, pulverization, melting or electronic sanitization. The method used will depend on the type of device as well as the nature of the information contained in the device. Such destruction methods require trained professionals and must be conducted by authorized personnel.

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 electronic records. The plan works in conjunction with this policy and the Media and Device Control Policy to ensure appropriate record management.

Record Retention Schedule – The established record type and timeframe for maintenance, retention and disposal of LADD records. This schedule may be deviated from with Steering Committee approval

A. ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	2 years
Bank Statements, Deposit Records and Canceled Checks	7 years
Employee Expense Reports	7 years
General Ledgers	Permanent

Record Type	Retention Period
Interim Financial Statements	7 years
Notes Receivable ledgers and schedules	7 years
Investment Records	7 years after sale of investment
Credit card records (documents showing customer credit card number) *	2 years
All service billing related documents	Current plus 7 years
All person supported billing related documents	Current plus 7 years

*Credit card record retention and destruction

1. All records showing credit card number must be locked in a desk drawer or a file cabinet when not in immediate use by staff.
2. If it is determined necessary to retain information on a document containing credit card information beyond 2 years, then the credit card number will be cut out of the document.

B. CONTRACTS

Record Type	Retention Period
Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination

C. GRANT RECORDS

Record Type	Retention Period
Original grant proposal	7 years after completion of grant period
Grant agreement and subsequent modifications, if applicable	7 years after completion of grant period
All requested IRS/grantee correspondence including determination letters and "no change" in exempt status letters	7 years after completion of grant period
Final grantee reports, both financial and narrative	7 years after completion of grant period
All evidence of returned grant funds	7 years after completion of grant period
All pertinent formal correspondence including opinion letters of counsel	7 years after completion of grant period
Report assessment forms	7 years after completion of grant period
Documentation relating to grantee evidence of invoices and matching or challenge grants that would support grantee compliance with the grant agreement	7 years after completion of grant period
Pre-grant inquiry forms and other documentation for expenditure responsibility grants	7 years after completion of grant period
Grantee work product produced with the grant funds	7 years after completion of grant period

D. INSURANCE RECORDS

Record Type	Retention Period
Annual Loss Summaries	10 years
Audits and Adjustments	3 years after final adjustment

Record Type	Retention Period
Certificates Issued to LADD	Permanent
Claims Files (including correspondence, medical records, injury documentation, etc.)	Permanent
Group Insurance Plans – Active Employees	Until Plan is amended or terminated
Group Insurance Plans – Retirees	Permanent or until 6 years after death of last eligible participant
Inspections	3 years
Insurance Policies (including expired policies)	Permanent
Journal Entry Support Data	7 years
Loss Runs	10 years
Releases and Settlements	25 years

E. LEGAL FILES AND PAPERS

Record Type	Retention Period
Legal Memoranda and Opinions (including all subject matter files)	7 years after the close of the matter
Litigation Files	1 year after the expiration of appeals or time for filing appeals
Court Orders	Permanent
Requests for Departure from Records Retention Plan	10 years
Compliance Related Documents (including complaints, investigations and work papers)	7 years
Service Related Audit Documents	7 Years
ORR and Licensing Investigations and Reports	7 years

F. MISCELLANEOUS

Record Type	Retention Period
Consultant's Reports	2 years
Material of Historical Value (including pictures, publications)	Permanent
Newsletters	Current version plus 2 years.
Policy and Procedures Manuals – Original	Current version with revision history
Policy and Procedures Manuals Copies	Retain current version only
Annual Reports	Permanent
Strategic Plans	Current Year plus 5 years.
Requests for Proposals	Current Year plus 5 years.

G. PAYROLL DOCUMENTS

Record Type	Retention Period
Employee Deduction Authorizations	4 years after termination
Payroll Deductions	Termination + 7 years
W-2 and W-4 Forms	Termination + 7 years
Garnishments, Assignments, Attachments	Termination + 7 years
Labor Distribution Cost Records	7 years
Payroll Registers (gross and net)	7 years
Employee Deduction Authorizations	4 years after termination
Time Card Data	Current plus 5 years
Unclaimed Wage Records	6 years

H. PENSION DOCUMENTS AND SUPPORTING EMPLOYEE DATA

General Principle: Pension documents and supporting employee data shall be kept in such a manner that LADD can establish at all times whether or not any pension is payable to any person and if so the amount of such pension.

Record Type	Retention Period
Retirement and Pension Records	Permanent

I. PERSONNEL RECORDS

Record Type	Retention Period
Commissions/Bonuses/Incentives/Awards	7 years
EEO- 1 /EEO-2 - Employer Information Reports	2 years after superseded or filing (whichever is longer)
Employee Earnings Records	Separation + 7 years
Employee Handbooks	1 copy kept permanently
Employee Medical Records	Separation + 6 years
Employee Personnel Records (including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	7 years after separation
Employment Contracts – Individual	7 years after separation
Employment Records - Correspondence with Employment Agencies and Advertisements for Job Openings	3 years from date of hiring decision

Record Type	Retention Period
Employment Records - All Non-Hired Applicants and selection files (including all applications and resumes - whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence)	2-4 years (4 years if file contains any correspondence which might be construed as an offer)
Job Descriptions	3 years after superseded
Personnel Count Records	3 years
Forms I-9	3 years after hiring, or 1 year after separation if later
COBRA	Current plus 7 years
Workers Compensation files	Current plus 10 years
Medical Records non-exposure	Current plus 7 years
Medical Records exposure	Current plus 30 years

J. PROPERTY RECORDS

Record Type	Retention Period
Correspondence, Property Deeds, Assessments, Licenses, Rights of Way	Permanent
Original Purchase/Sale/Lease Agreement	Permanent
Property Insurance Policies	Permanent

K. TAX RECORDS

General Principle: LADD must keep books of account or records as are sufficient to establish amount of gross income, deductions, credits, or other matters required to be shown in any such return. These documents and records shall be kept for as long as the contents thereof may become material in the administration of federal, state, and local income, franchise, and property tax laws.

Record Type	Retention Period
Tax-Exemption Documents and Related Correspondence	Permanent
IRS Rulings	Permanent
Excise Tax Records	7 years
Payroll Tax Records	7 years
Tax Bills, Receipts, Statements	7 years
Tax Returns - Income, Franchise, Property	Permanent
Tax Workpaper Packages - Originals	7 years
Sales/Use Tax Records	7 years
Annual Information Returns - Federal and State	Permanent
IRS or other Government Audit Records	Permanent

L. CONTRIBUTION RECORDS

Record Type	Retention Period
Records of Contributions	Permanent
LADD's or other documents evidencing terms of gifts	Permanent

M. PROGRAM AND SERVICE RECORDS – see

https://www.michigan.gov/documents/dtmb/RMS_GS20_640204_7.pdf

Record Type	Retention Period
All Records for Individuals- 20.0059	10 years
Identification Face Sheets, Diagnosis and Discharge Summary- 20.0058	20 years after discharge
Programmatic Records (HIPAA Log, Emergency Drills, –Employee Training Book, Maintenance Records, IRs)	Current year plus 2 years.
Fees	7 years
Medical Records	7 years
LADD convening reports (meetings)	Permanent (1 copy only)
Research & Publications	Permanent (1 copy only)
All Records for Individuals Who Lived in a Licensed Setting and Have Been Discharged	2 years of records prior to the date of discharge kept at the home

N. FISCAL SPONSOR PROJECT RECORDS

Record Type	Retention Period
Sponsorship agreements	Permanent

O. COMPANY RECORDS AND RESOURCES

Record Type	Retention Period
Board of Directors- past and current information	Permanent
By Laws	Permanent
Annual Financial Reports	Permanent
Equipment Inventory	Current plus 7 years
Administrative Subject Files (analysis and planning documents)	Current plus 6 years
Hazardous Materials Safety Data Sheets	Current plus 30 years
Planners and Calendars	Current plus 2 years
Audio-Visual Material	Current

PROCEDURE FOR STORAGE AND DISPOSAL OF PERSON OR COMPANY ASSETS

Seasonal Clothing

Seasonal clothing for each person should be stored at the program unless there is no area available. If no area is available the Area Supervisor will coordinate storage on an individual basis, considering the most efficient and practical option. Clothing items for storage will be placed into sealed totes (mothballs are optional and may discourage pests). Label the tote on the outside with Large Block Print. Label by

- a. Program Name
- b. Person's Initials

If a person's clothes are damaged, no longer fit or are clearly unwanted follow the process for documenting disposal as outlined on the Personal Belongings Inventory form located in individual Personal Allowance Books. This form states, "**2 staff must sign when any items purchased with personal funds are brought into the program or when any personal belongings leave program except for usual daily wear and disposable personal items.**" and must be coded according to the form as follows;

Method of Removal

- a. Destroyed by self = D/S
- b. Destroyed by some other mechanism = D/M
- c. Destroyed due to lack of fit = D/F

Furniture, Medical Equipment, Televisions, Appliances and Washers and Dryers

Any furniture, medical equipment, televisions, appliances or washers and dryers owned by the **people** must be listed on the Personal Belongings Inventory form located in individual Personal Allowance Books. If it is determined an item is no longer usable or wanted the following will occur:

- a. With Management assistance, the person or guardian will provide documentation to be put in the person's Personal Allowance Book, which states the item and how they would like the item disposed of. If the item is to be sold, a price must be included as well.
- b. Based on the noted disposal, the Supervisor will coordinate to have the item removed from the program and disposed of.
- c. If the item is to be sold, the Supervisor will obtain documentation of fair market value by using an available resale website such as Craigslist or Let Go to verify the price for the item requested is reasonable. Documentation of the price must be kept in the person's Personal Allowance Book along with the documentation of the person or guardian disposal request.
- d. If necessary, the Supervisor will assist in the sale of the item.

Any furniture, medical equipment, televisions, appliances or washers and dryers owned by **LADD** must be listed on the Equipment-Appliance List and/or the Major Equipment and Furnishings List located in the Maintenance Manual. If it is determined the item is no longer usable, the following will occur:

- a. If the item is to be disposed of, the Supervisor will document the items removal from the Equipment-Appliance List and/or the Major Equipment and Furnishings List located in the Maintenance Manual.
- b. The Supervisor will coordinate to have the item removed from the program and disposed of.
- c. If the item is usable the Supervisor will coordinate with the Maintenance Department to put the item into long term storage as follows:
 1. The item will be taken to the Hillside pole barn, or if the item requires protected storage due to vulnerability to infestation or leaks, it is to be taken to the Hillside basement.
 2. The Area Supervisor must coordinate this storage and any special instructions for storage. Assistance with pick up/delivery and keys will be necessary to complete the process.
 3. The item will be tagged with the County and Program Name.
 4. The Maintenance Department will keep an inventory of items in long term storage
 5. If an item is needed, the Supervisor will coordinate with the Maintenance Department to obtain the item and the item will be removed from the inventory.
 6. If necessary, items from the Central Region can be stored in these locations as well. In this case, the Director will coordinate arrangements.

*****LADD IT Assets*****

All LADD IT assets are inventoried and disposed of in accordance with the Device and Media Control Policy.

PROCEDURE FOR PURGING AND STORAGE OF COMPANY AND STAKEHOLDER RECORDS

Personnel Records:

Personnel records are stored and organized as outlined in the Recruiting, Application and Hiring Policy. Employees hired prior to 2016 have a paper personnel record. Employees hired 2016 and forward have both a paper file and an electronic file in the Filehold system. Once an employee is termed, if they have a paper record, all portions of their files are banded together, kept in the HR Records Room and then transferred to storage containers by year of termination before being moved to longer term storage. If the employee had their record in Filehold, it will be retained per the record retention table. Regardless of hire date, all active Management personnel records are kept in paper form and locked in a separate and secure location. Personnel Records will be stored in long-term storage by the Human Resource Department according to year termed.

Company and People Supported Records:

All company and people supported records are purged according to the details outlined in the Purge Grid document associated with this Policy. Documents in three ring binders or in plastic sleeves must be removed from such. The designated storage location for all records is the Niles long term storage building.

- a. The Quality Assurance Department will transfer company QA records into individual containers and label accordingly. Arrangements will be made to take the records to long term storage. People supported records will be secured according the Purge Grid and arrangements will be made to take the records to long term storage.



LADD

WE MAKE THE DIFFERENCE

Program/Person Purge Grid

Book Name	People Supported Material (What items are being Purged)	Monthly	Over 1 year old (can be purged to a banks box and kept on site)	Over 2 year old (can go to long term storage)	Over 10 year old
Goals and Objectives Book	Any paper form of documentation or relative information associated with the following items. If any of the following have any written enteries they would get purged. Goals and Objectives Data Sheets. Daily progress notes. Behavior Treatment Plan Data Sheets /ABC charts. Sleep charts. LADD Community Outing Log	Purge in persons purge book	More than 1 full year old purge in person's box.	Anything more than 2 full year old purge into a person's box.	Compliance arranges termination of outdated records.
Goals and Objectives Book	Purge any paper document or relative information associated with the following items. PCP Person Centered Plan and Addendums- (Contract Agency & L.A.D.D., Inc.) Personal Profile. Behavioral Treatment Plans. Employee Training Signature sheet. Items purged from the Goals Book annually when a new PCP goes into effect. Specific trainings or inservice documents pertaining to a person		More than 1 full year old purge in person's box (PCP, Behavioral Plans, don't purge old one until the new one is in place).		
Medication Book	Purge any paper document or relative information associated with the following items. Medication Records, Treatment Sheets, Count Sheets and Protocol Order records. Bowel Movement Record, Menses Chart (If applicable). Vital Signs records and Seizure Chart (If applicable).	Purge in persons Aministrative records book			
Medication Book	Purge any paper document or relative information associated with the following items. Persons Standing Missed Mediation Orders and Protocol Orders. Consent for Psychotropic Medication. Old Prescriptions (expired or discontinued). Administering Medication signature sheet.				
HCC Book	Persons HCC Sheets				
Administrative Records Book	Documents to purge: Persons Personal Profiles etc., PCP, Addendums. Supports Coordinator Notes. MAIR, Heath Care Plan, Nursing Annual Assessment Etc. Annual Physical (Health Care Appraisal, keep 2 year worth in book), TB Test and results, only purge when there is a new one in place. Lab and X-ray results. Mammogram, PAP/Prostate, Podiatry (If applicable). Neurology, Seizure Records (If applicable). Monthly Weights (previous year's weight records), Dietary/Nutrition Assessment (If applicable). Dental, Vision, Speech, Swallow, Audio logical – Hearing. (If applicable). Occupational Therapy, Physical Therapy (If applicable). Medication consent for Psychotropic (originals). Behavior Management Information. (If a person's BTP or Guidelines are discontinued, note on the top of the plan the date that it was discontinued, this would not get purged out unless there was a new one in place that would replace the old). (Only Purge Documents that have a new one to replace the old, (For example someone has a Dietary/Nutrition Assessment and it was completed in 1998, no additional assessments were needed). That Assessment will stay in the Records Book indefinitely or until a new one is in place and replaces the old).		Only purge items that are: over 1 year old and have a new form to replace the old. More than 1 full year old purge in person's box (Note: please make sure you don't remove a permanent document).	Only purge items that are: over 2 year old and have a new form to replace the old. Purge in person's. (Note: please make sure you don't remove a permanent document).	Compliance arranges termination of outdated records.

Incident Report Book	IRs			2 year, plus current working year of IR's are kept on site. Anything older than that purge in person's box.	Compliance arranges termination of outdated records.
Personal Allowance Book	Persons Personal Allowance Ledgers.	Annual	More than 1 full year old purge in person's box box.	Anything more than 2 full year old purge in person's box.	
Discharge from LADD Services	All documents for that person, pack in bankers box, label with name and year for long term storage.	when applicable			
Book Name	Program Material (What items are being Purged)	Monthly	Over 1 year old (can be purged to a banks box and kept on site)	Over 2 year old (can go to long term storage)	Over 10 year old
HIPAA Log	Section II		More than 1 full year old purge in program box.	Anything more than 2 full year old purge in program box.	Compliance arranges termination of outdated records.
Maintenance Manual	Section I-III Purge Annually, Section IV Purge every two year		Section I-III Purge Annually Anything more than 1 full year old purge in program box.		
Employee Training Book	Section I Miscellaneous Training, Section II Family Staff Information.		More than 1 full year old purge in program box.		
Staff Communication Book	Staff book notebooks/pages, shift duties, postings and other.	Every six months can purge to a program purge box.			
Menu Guide	Substitution sheets, old menu sheets				
Resident Register Service Register	N/A	Do Not Purge	N/A	N/A	N/A
Service register Resident Register	N/A	Do Not Purge			
Toolbox Book	Do Not Purge. The only time you would purge sheets from the toolbox training book is if there was person specific information and that person was no longer there or if there was a change and person specific information was updated. If that occurs the document would get purged in the persons purge.	Do Not Purge	N/A	N/A	N/A
Vehicle Log (Mileage)	Vehicle Mileage Log	Monthly, West Office, Print Room, in appropriate box.	Compliance will relocate to long term storage annually.		Compliance arranges termination of outdated records.
Petty Cash Book	Petty Cash Funds Ledger Printout		More than 1 full year old purge in program box.	Anything more than 2 full year old purge in a program box.	
Emergency Guidebook	Emergency Guidebook, Drills and Drill Data Sheets, Any worksheet that is outdated and has been replaced with a newer updated one. Scores must be kept in book until new one is completed each year to replace previous one. Unless there was a change that prompted additional Scores to be completed in which case you would keep both versions in the book for the year.		More than 1 full year scan all drill logs into manager (R) 007 Emergency Forms and then put paper copies in old purge in program box.	Anything more than 2 full year old purge in a program box.	



NON-DISCLOSURE AGREEMENT

The undersigned, as a condition in consideration of being permitted to view protected health information (PHI) and tour a program where Living Alternatives for the Developmentally Disabled Inc. provides staffing supports and maintains PHI agrees as follows:

1. That all information obtained on said premises shall be and will remain confidential, and shall not be disclosed to any third person, firm, or corporation except as permitted in writing by an authorized agent of Living Alternatives for the Developmentally Disabled Inc. and except to the extent that such information does not and cannot identify any person served, group of people served, or otherwise constitute disclosure of any particular disability, treatment, or other medical or personal information.
2. That no photographs, drawings, names, or other means of identifying the people we serve may be taken while on the premises, without specific written permission from an authorized agent of Living Alternatives for the Developmentally Disabled Inc.
3. This agreement may be enforced by Living Alternatives for the Developmentally Disabled Inc. and/or any affected person served by an action for an injunction, or damages, or both.

Print Name

Signature

Corporate Compliance Officer Signature

Date

Date

WE MAKE THE DIFFERENCE



CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

LADD through the course of operations, produces and maintains several types of sensitive, confidential protected health information for the people we support and personal employment related information for our employees. It is important to protect the interests and rights of LADD and our stakeholders and the information they have entrusted to us at all times. Individual and business privacy are governed by series of Federal Privacy Laws and enforced by federal agencies such as the Department of Labor, Office for Civil Rights and Department of Health and Human Services. LADD maintains strict compliance with all applicable standards and requires all Business Associates, short term contractors and consultants to do the same.

Information, for purposes of this Agreement includes but is not limited to the following

- All LADD Policies, Procedures and forms in hard copy or electronic formats.
- Any and all portion of the Personnel File in hard copy or electronic formats.
- Any person supported information in hard copy and electronic formats as noted in the LADD Compliance and Ethics Program and the HIPAA Security and Safeguard Policy, full version available upon request or a condensed version can be found at www.laddinc.net.
- Any and all conversations of a confidential nature.

This Agreement is intended to prevent the unauthorized disclosure of Information as defined above. A violation of this agreement could lead to criminal and/or civil penalties by signing this Agreement the signor acknowledges understanding and agreement with the terms and conditions and maintains that they will protect the interests and rights of LADD and our stakeholders at all times.

Print Name

Signature

Date

Corporate Compliance Officer Signature

Date

WE MAKE THE DIFFERENCE



CONFIDENTIALITY AGREEMENT

LADD PERSONNEL

While working in the LADD Office or in locations operated or staffed by LADD access to and knowledge of sensitive, confidential information will occur routinely in the course of completing my job responsibilities. This information relates to employees and/or people supported and consists of demographic, personal, medical, insurance, financial, legal, and clinical information.

Release of this confidential information, either written or verbal, except as required by your job responsibilities is a **critical violation of the LADD Compliance and Ethics Program (CEP) and may be a violation of the law and professional ethics.** Failure to comply with the CEP may be reason for disciplinary action including separation from employment.

I understand that I should only access and review information within the scope of my job responsibilities and accept my responsibility to protect the confidentiality of all people supported and employee information. I will limit distribution of confidential information to only parties with a legitimate need and right to know.

I understand that if, during the course of my employment, I encounter sensitive, confidential information regarding an employee or person supported that I must preserve the confidentiality of that information. All confidential information and work papers are the property of LADD and therefore must never be photographed, copied or removed from the office or any other staffing location without following the LADD CEP. All paper and electronic documentation are considered confidential and must be properly disposed of according to the Record Retention and Asset Management Policy. I understand that working in the LADD Office or in locations operated or staffed by LADD that if I need to discuss confidential issues regarding employees or people supported I will ensure this is done in a private setting. I will only communicate with positive intent and follow the Mission, Vision and Values at all times throughout my employment at LADD.

I further understand that I may be disciplined if I knowingly violate any of the confidential obligations according to the CEP. I further understand that even if removed from my employment with LADD or if I terminate my employment voluntarily, these confidentiality obligations continue to apply to any information I have already had access to during the course of my employment.

I have read, understand and agree to abide by this Agreement as a condition of my employment.

Employee Signature

Date

Management Signature

Date



ALL STAFF – MUST READ

Because LADD provides health care services, all employees are required to follow the HIPAA guidelines to safe guard and secure protected information of the people we support, which includes visits or calls by former employees.

Therefore, any employee leaving LADD's employment is not allowed back on the premises unless they are an approved Natural Support. Only Administration, in conjunction with the Guardian, can approve a Natural Support.

Former employees are not allowed to receive any information about the people supported, LADD employees, or the organization at any time, through any means (face to face, phone, meetings in community etc.).

The following employee, _____, is no longer working for LADD and therefore, is not allowed on the premises, and the above information applies. The employee named above is also not currently an approved Natural Support.

Former employees are made aware that they are not allowed on the premises so this should not be a problem. However, if the former employee named above tries to call for information and/or tries to visit; staff are not to give any information and/or open the door; i.e. allow them into the home.

Due to the important service we provide, staff must call the local police department to inform them that the former employee is not following these requirements, and it is considered to be trespassing.

Former employees know that they are always welcome to call the Executive Director, Julia Jeffreys; if they have a disagreement with the above directive.

Thank you for following this required procedure!!



EMPLOYEE STANDARDS OF CONDUCT

At LADD the standard for all employees is to provide for a respectful, safe, efficient, accessible and positive environment for the people we support and for all co-workers.

The CEP provides detailed guidance for all employees regarding expectations for acceptable behavior. Honesty and integrity are an employment requirement along with respectful, positive communication. All employee must understand these expectations and responsibilities and that violations of these standards will lead to corrective action up to and including separation from employment.

Any time an employee has a question or needs clarification regarding standards and best practice it is their responsibility to seek out a member of management and obtain an answer.



LADD

WE MAKE THE DIFFERENCE



STANDARDS OF CONFLICT

PURPOSE

To establish standards for all LADD employees, which provide for a respectful, safe, efficient and positive environment and are accessible and available so that all employees are fully informed of expectations and their responsibilities.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to set and establish standards for the guidance of all employees regarding expectations for acceptable behavior. The following represents only a partial list of unacceptable behaviors and conduct; a complete list of all possible violations would be impossible to write.

STANDARDS AND DEFINITIONS

Honesty and integrity are an employment requirement. Violations will lead to corrective action up to and including separation from employment.

BREACHES OF STANDARDS OF CONDUCT

1. Abuse, mistreatment or neglect of the people we support.
2. Borrowing items or money from the people we support.
3. Violating the boundary between employee and person(s) supported in any way. (Including but limited to inappropriate names, touching, etc.)
4. Falsifying documentation for services, employment application, time keeping, personnel, or other company documents or records.
5. Unauthorized possession or use of company or employee property.
6. Gambling, carrying weapons or explosives, alcohol, drugs, or violating criminal laws on company premises and/or during work hours while providing support services within a location.
7. Fighting, throwing things, horseplay, practical jokes or other disorderly conduct, which may endanger the well-being of any person supported, employee or company operations.
8. Engaging in acts of dishonesty, fraud, waste, abuse, theft or sabotage.
9. Being under the influence or possession of alcohol or illegal substances on company property and/ or during work hours while providing support services within a location.
10. Using the company vehicle for personal use.
11. Engaging in sexual intercourse or other sexual behavior while on company property and/ or during work hours while providing support services within a location.
12. Threatening, intimidating, coercing, using abusive or vulgar language, or interfering with the performance of other employees or person(s) receiving support services.
13. Insubordination or refusals to comply with instructions or failure to perform reasonable duties which are assigned by a member of Management.
14. Unauthorized use of company material, time, equipment or property.
15. Damaging or destroying company property or person(s) supported's property through careless or willful acts.
16. Conduct, which the company feels, reflects adversely on the employee or company.
17. Performance which, in the company's opinion, does not meet the requirements of the position.
18. Engaging in such other practices as the company determines may be inconsistent with the ordinary and reasonable rules of conduct necessary to the welfare of the company, its employees or the people we support.
19. Negligence in observing fire prevention and safety rules.
20. Other circumstances for which the company feels that corrective action is warranted.
21. Witnessing or signing legal documents without direction of supervisor.

This list is intended to be representative of the types of activities which may result in corrective action. It is not intended to be comprehensive and does not alter the employment-at-will relationship between employees and the company.

PROCEDURE

There is no progressive discipline policy.

1. Corrective action will be determined on a situational basis and approved by Administration.
2. The Employee Code of Conduct Handbook provided is available to review for employment expectations.
3. LADD Employee Policies and Procedures are available to review for employment expectations.
4. Separations from employment are approved only by the Executive Director.



LADD

WE MAKE THE DIFFERENCE



CONFLICT OF INTEREST – CODE OF ETHICS POLICY

PURPOSE

This policy is designed to assist employees to identify situations that present potential conflicts of interest, to protect LADD interest when contemplating these situations, and to outline a procedure by which the organization will address potential conflict. This policy is intended to supplement but not replace any applicable laws.

SCOPE

This policy applies to all LADD employees and volunteers.

POLICY

It is the policy of LADD to promote a positive public image that aligns with the Mission, Vision and Values of the company. All activities will be transparent and conducted in a manner that is free of perceived, potential or actual conflicts or ethical violations. Should such conflicts or violations arise a reporting mechanism as well as a system of documenting appropriate resolution will be followed.

STANDARDS AND DEFINITIONS

Principles of ethical behavior are found in the Values of the company and are carried over into the Core Competencies of every job description. Ethical behavior is demonstrated in many ways such as;

- Stand in Truth – Work and communicate with honesty, integrity and openness; having a willingness to improve qualities in self and the organization; and seeing all people as equal.
- Remain compassionate – Demonstrate kindness in action towards others, promote self-confidence and self-esteem and appreciate differences in people.
- Take responsibility – taking ownership for the decisions we make or fail to make, the actions we take or fail to take, and the consequences that result.
- Give respect – it is our duty to show a high regard for ourselves, others, and the resources entrusted to us. Resources entrusted to us may include people, money, reputation and the safety of others.
- Remain honest – it is critical to understand the truth and act in a truthful manner both in our communications and in our conduct. Our conduct must be free from competing self-interest, prejudice, and favoritism.

A conflict of interest exists if circumstances would lead a reasonable person to question whether motivations are aligned with LADD's best interests. It is important to understand that a conflict of interest can occur;

- When an employee or their relative is in a position to benefit personally, directly or indirectly, from his or her relationship with a person or entity conducting business with LADD the potential for a conflict exists; and therefore, must be scrutinized. All employees have an obligation to avoid conflict, or the appearance of conflict, between their personal interests and the interests of LADD and not allow their impartiality to be questioned. Administrative review and/or Board review must take place in order to prevent conflicts.

Conflicts are typically characterized as;

- Ethical – a decision is made or action is taken that is contrary to company policy and puts the company at risk or serves to undermine the integrity of company.
- Legal – a decision is made or action is taken that violates a law, regulatory standard, contract or agreement and puts the company at risk for possible criminal or civil penalties.
- Financial – a decision is made or action is taken that involves financial gain or risk at the expense of the company, jeopardizes financial solvency of the company or unduly impacts a contract or agreement.

Overview of areas where conflict or ethics violations can occur;

- Kickbacks and Gift Receiving for Personal Gain – Employees must be cautious of gifts that may be given with the intent to influence care or services provided, and accepting such gifts have the potential to create conflicts of interest. Employees provide high quality services at all times.
- Loans – Borrowing or loaning cash or objects of value including company property can create a situation of inequality where repayment, reimbursement or recompense is conditional with one party having power over the other as part of the transaction.
- Political Activities – Activities completed as an individual and on personal time must clearly make a distinction that during these activities the individual is not a representative of LADD and is not using LADD materials, equipment or locations for their activities.
- Recreation and community activities – Participation in events and activities must be at the request or agreement of the person supported and/or their family. These activities make use of the person's and the company's funds and the potential for involvement in activities and expenditures that benefit a LADD employee over the person supported. Activities should be well thought, planned and approved.
- Paying a person receiving supports to do work – First and foremost involve issues of recipient rights if the person is not legally employed. Possible ethical concerns and conflicts can arise depending on the type of work, number of hours work is performed, the rate of pay and working conditions. All of these areas present substantial risk to the company and individuals and should be well thought out, planned and approved.
- Harassment and workplace violence – When situations are considered to be harassing or threatening in nature or make the working environment uncomfortable they should be reported immediately. Once reported the situation must be addressed immediately, according to policy. Failure to act can result in allegations of conflict of interest and ethical concerns. These issues must be reported to the Human Resource Department immediately and preferably within 10 days from the event.
- Promotions – Must be made in compliance with company policy which states candidates are selected based on their skills and experience and are the best matched for the needs of the company. Failure to do so can result in allegations of conflict of interest and ethical concerns.
- Solicitation – Distribution of written material by employees or non-employees during work hours and in work areas i.e. pamphlets, booklets, newsletters and handbills have the potential to shape opinion, promote or discourage a position can present the possibility of undue influence; and therefore, are prohibited. Solicitation facilitated through telephone or electronic communication systems; other solicitations through LADD telephone or computer/electronic systems are prohibited.
 - ❖ Verbal or written solicitation by employees or non-employees enjoining members to join, enlist or in any way become a part of any organization during work hours in work areas is prohibited. Organizations include, but are not limited to those generally defined as fraternal, social, religious or political.
- Sales and fundraisers – Raffles, charity drives, sports pools, cosmetic or jewelry sales, bake sales or the sale of any other item that has the purpose of raising cash or anything of value for the seller can result in unwanted pressure to the buyer where they feel an obligation to purchase or participate creates a situation of inequality; and therefore, must be approved by the Guardian and Administration.
- Outside employment – An employee who has an obligation to another employer creates a situation where the employee may act in the interest of the other employer over LADD. Outside employment by salaried on call employees must be reviewed by Administration.
- Supervising the work of someone with whom you have a relationship – Situations where an employee reviews, approves or controls a contractual or business relationship between LADD and someone the employee has a relationship can be a conflict of interest. An employee who supervises reviews, determines compensation or assigns work to a family member can create a conflict. In these circumstances' steps must be taken to demonstrate transparency, fairness, impartiality and objectivity. Steps taken need to be approved by the Human Resource Director, Steering Committee and/or Executive Director/ Board of Directors.

Upon separation from employment increased monitoring of relatives still employed may occur to assist with the mitigation of risk to the organization.

If an employee suspects a violation of this policy it should be reported immediately per the Complaint Reporting Policy. Additional reporting information is also available on the LADD website. The Whistleblowers Policy will be strictly adhered to at all times in the application of this Policy.





CELL PHONE AND TEXTING POLICY

PURPOSE

The purpose of the Cell Phone and Texting Policy is to provide guidance to employees so they understand their first responsibility is in meeting the needs of the people we support at all times, and not to receive/respond to extensive personal non-emergency calls/texting and accessing applications or the internet while at work using their cell phone.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to ensure a means of communication is available at all time in the staffing locations and vehicles. It is the job responsibility of all employees to ensure the needs of the people we support are met at all times and the personal use of cell phones and other devices used for communication do not interfere with this responsibility.

STANDARDS AND DEFINITIONS

- ❖ **Devices for taking pictures of people supported and/or capturing any information is prohibited by employees to ensure HIPAA compliance. Therefore, taking pictures of the people supported with cell phone cameras is prohibited. In addition, taking pictures of work papers, confidential information and records of any kind is strictly prohibited. Violations may result in separation from employment.**
- ❖ **Texting of confidential information is prohibited. No information, including the person supported name or any other identifying information covered by the HIPAA Privacy Rule will be texted by employees. Text messages are not encrypted and are a violation of this policy.**
- ❖ **No calls, texting, or emailing are to occur while driving any vehicle. When necessary 911 calls must be made once the vehicle is safely on the side of the road.**
- ❖ **LADD provides telephones and internet service in staffing locations for the personal use of the people who reside there and for daily operations. Cell phones are provided in the vehicles for emergency purposes.**
- ❖ **Program, employee, and Management telephone numbers either home or cell numbers should never be given out except to current employees of LADD. If necessary, take the callers information and pass it along to Management.**

****Note – Use the Program phone to make an emergency call so the 911 system can automatically track the location of the call to dispatch emergency personnel more readily. *****

PROCEDURE

1. An employee's primary duty while on shift is the safety and well-being of the people served. Cell/telephone calls, texting, emailing and/or internet or use of any other communication devices must not interfere with this duty. The use of all headsets, Bluetooth devices, or any other devices that may limit or impair hearing is a safety risk and is therefore prohibited.
2. If at any time, communication devices interfere with an employee's primary duty; use will be restricted by Management. This may include excessive calls, texting, use of social media websites etc.

3. Employees must keep personal calls to a minimum. Personal calls must not exceed 3 minutes or interfere with the safety and well-being of the people supported, and could constitute as neglect. Long distance calls are prohibited. Home telephone numbers or cell phone numbers should never be given out except to current employees of LADD and if listed at your work location.
4. Numerous interruptions at work and/or over use of cell phones may result in Management prohibiting the cell phone at the work location.
5. Excessive phone/electronic device usage or phone calls over 3 minutes are considered a violation of the rights of the people supported and disciplinary action up to and including separation from employment may occur. All Employees are required to follow the standards of telephone usage, which gives a time limit of up to 3 minutes, and this includes use of their own personal cell phone for talking, texting, emailing and/or internet.
6. If at any time the care of the people we serve is being negatively affected, Management will not allow employees to bring their cell phones into the work place.
7. If it has been determined that your program location is no longer allowing employee cell phones on the premise and you are an employee who is experiencing a situation in which s/he feels the need to have a cell phone at work due to medical or other issues; the employee must contact the Human Resource Department for review and approval for use.
8. Employees have permission to make local calls or receive calls of up to 3 minutes at their work location with the phone that is available. Any calls resulting in an additional phone bill charge will be the responsibility of the employee to pay.
9. Lengthy calls or numerous calls while on shift negatively affects the care of the people we support; and therefore, is prohibited.
10. Excessive sending and receiving of text messages is viewed the same as lengthy or numerous calls and is prohibited as well. This includes employees own personal cell phones used for voice calls or texting.
11. Violations of this policy must be reported to a member of management for further action.



LADD

WE MAKE THE DIFFERENCE



SOCIAL MEDIA POLICY

PURPOSE

Social media communications must align with the LADD Mission, Vision and Values. The LADD Social Media Policy establishes guidelines for employees to conduct social media engagement in both official and unofficial capacities, promotes a safe environment for sharing information and protection from violation of applicable regulations or laws.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to establish a framework for employees to make responsible decisions about their use of social media in order to meet job responsibilities and LADD business interests are not negatively affected.

STANDARDS AND DEFINITIONS

Social Media – includes but is not limited to, all means of communicating or posting information or content of any sort on the Internet, including the following forums: blogs, podcasts, discussion boards, on-line collaborative information and publishing systems that are accessible to internal and external audiences (i.e., wikis), RSS feeds, video sharing, personal websites, and social networks such as but not limited to Facebook, Twitter, Snapchat, Instagram, TikTok, YouTube, as well as all other social media forms.

LADD recognizes the use of various online communities and the need to outline the expectations and responsibilities of employee's use of social media networks and internet-based communications. Such communications may include, but are not limited to accessing, using, posting, publishing, or monitoring online sites, forums, blogs, wikis, or video logs (e.g., Facebook, Twitter, Instagram, LinkedIn, Tik Tok, YouTube, blogs, media sites and other similar online venues). The purpose of this policy is not to restrict an employee's protected activities under Section 7 of the National Labor Relations Act. It is to follow and uphold LADD's MVV.

LADD fully respects the legal rights of our employees including their rights under the National Labor Relations Board to engage in concerted and protected activities. If at any point this policy or parts thereof are determined to interfere with the legal rights of employees then the rights of the employee will take precedence over the policy.

PROCEDURE:

1. While it is each individual's decision whether or not to use social media networks, employees should always be aware that their behavior and opinions may reflect on LADD.
2. Social media networking and internet-based communications by employees should be consistent with applicable laws and LADD policy.
3. **Employees shall not publish, discuss or reference confidential information about any person receiving services including health information or information otherwise protected by HIPAA. This includes a person's name, photographs, videos within their home, diagnostic testing results and images, case information, or any information that may lead a reasonable person to be able to identify a person supported.**
4. Employee communications on social media networks or online communications should not contain information that identifies a person served identity or condition.
5. Employees shall respect the privacy rights of other employees, person's supported, contract agency and people in the community of LADD by refraining from writing about or sharing information that may be considered a breach of privacy or confidentiality. Employees shall not publish, post, or discuss other people's personal information.

6. Employees have a right to their personal privacy. They have the right to keep their personal opinions, beliefs, thoughts and emotions private. Employees are prohibited from sharing anything via social media channels that could violate another employee's right to personal privacy.
7. Employee communications must not contain LADD confidential, proprietary or trade secret information. This includes information about trademarks, sales, financial information, number of employees, salaries, person supported information and data, LADD strategy and financial information, information provided to LADD by third parties, or any other information that has not been publicly released by LADD. These are examples only and do not cover the full range of information that may be considered confidential and proprietary. Employees should refrain from using LADD's name and/or logo or trademarks when using social media networks or online communications.
8. Each individual employee, professional, volunteer or other associate of LADD or its affiliates is personally responsible for his or her content on social media networks and other online communications.
9. Any communications should reflect an individual's personal point of view only and must not be presented as the viewpoint of LADD.
10. Employees shall not represent, claim or imply that they are speaking for, or representing LADD. The content should be clear that such communications are the individual's personal opinions and do not reflect the opinion of LADD or its affiliated entities.
11. If employees, professionals, volunteers or other individuals associated with LADD acknowledge their relationship with LADD in an online community, they shall include disclaimers in their online communications advising that they are not speaking officially on behalf of LADD.
12. Employees are solely responsible and liable for the content they post or publish and LADD shall not be liable for any errors, omissions, losses or damages claimed or incurred due to any content posted or published by an employee. We encourage employees to use the LADD Mission, Vision, and Values to help guide them in their actions and words.
13. Employees are reminded content or information posted and published remains available for indefinite periods of time.
14. Before posting or publishing, content should be considered carefully and caution should be exercised. Employees should exercise good judgment and strive to be accurate, fair and responsible when using social media networks and should be respectful and professional to fellow employees, supervisors, and LADD. Following the LADD Mission, Vision, and Values will help you to communicate in a positive, open, effective manner.
15. Employees and others associated with LADD may not post or publish disparaging material that is libelous, slanderous, or defamatory which identifies LADD, administrators, managers, supervisors, employees, or people supported/families, which is false and damages their reputation.
16. Employees need to be aware of their relationship to LADD in all social media disclosures. Nothing gains more notice in social media channels than honesty or dishonesty. Employees who have a vested interest in something they are discussing, should acknowledge that relationship and point it out, so long as they can do so without forfeiting their legal rights to engage in concerted or protected activities related to their employment.
17. Employees are encouraged to use LADD's numerous options for employees to ask questions, make comments/give feedback and suggestions for improvements in the most efficient and effective manor via Corporate Compliance, Quality Assurance, and/or contacting members of Management directly instead of posting information via electronic communications. Solutions to employment problems can be addressed using LADD options whereas electronic postings offer no solutions.
18. Employees shall not access, use, post, publish, or monitor any social media network or online communication forum while at work at LADD, whether through personal communications devices, such as laptops, cell phones, smart phones, PDAs, or other similar devices, or while on LADD computers or tablets, unless expressly authorized to do so for LADD purposes.
19. Employees shall not download, install or use social media network software on LADD computers or tablets.
20. Employees are responsible for understanding and being aware of the LADD policy on Harassment and Violence at the workplace found in the Handbook Code of Conduct and LADD Directory, and how those policies affect an employee's use of social media.

21. Employees may be disciplined, up to and including termination, by LADD for communications, commentary, or images that violate this policy.
22. Social media tools are becoming increasingly important in local and incidental crisis and emergency management communications. Nevertheless, even in times of crisis, disaster or emergency, only employees with the authority to speak on behalf of LADD are permitted to do so.
23. LADD reserves the right to monitor, restrict, block, suspend, terminate, delete or discontinue access to any work-related social media network sites without notice and at its sole discretion.
24. 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.



LADD

WE MAKE THE DIFFERENCE



FUND RAISING POLICY

PURPOSE

This policy is designed to assist employees to understand the process for fundraising.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to engage in fund raising activities that create opportunities to benefit the people supported, educate the public regarding LADD and demonstrate our commitment to good community relations. Strict oversight and accountability will be maintained to ensure all fundraising is completed in compliance with all applicable laws and regulations.

STANDARDS AND DEFINITIONS

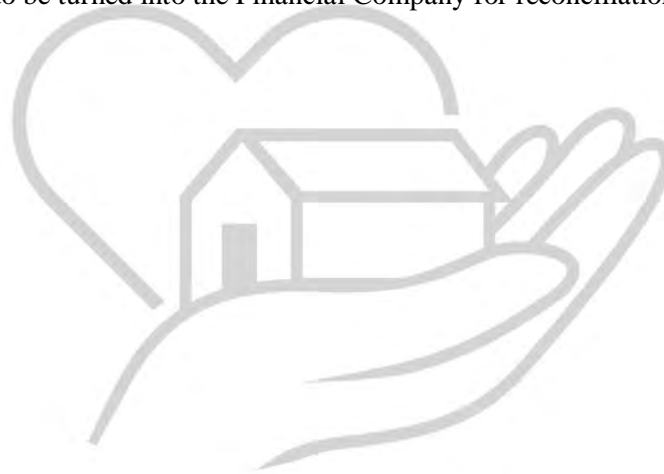
Personal gain fundraising is not permitted. Each request for fundraising activities will be handled on an individual basis and must be made prior to any solicitation. Failure to obtain permission will result in disciplinary action up to and including separation from employment. Examples of personal fund raising include personnel soliciting funds on behalf of a personal cause, selling cookies for a child or family member in girl scouts, selling candy or wrapping paper for a child or family members school, having persons supported selling items on behalf of the organization, allowing persons supported to raise funds by appeals to personnel or other persons supported.

Employees are not allowed to sell items (i.e. Avon etc.) to the people we support.

PROCEDURES

1. **Prior approval for all fundraising must be obtained.** All Fund Raisers must be with reputable companies/organizations. The Executive Director or their designee must be made aware and authorize any fund-raising activities or the intent to solicit funds.
2. All Fund Raisers must have a designated lead/responsible person who is responsible for all aspects of the Fund Raising including the funds collected. The designated lead can be a volunteer or designated by committee as outlined in #3 below.
3. A Fund-Raising Committee may be established to aid in the fund-raising process.
 - a. Fund Raising Committees will have a designated chairperson as agreed upon by the group.
 - b. The Committee's designated chairperson will be responsible to ensure the appropriate approval and feedback have been obtained for Committee projects, prior to moving forward with any fundraising projects.
 - c. Committee responsibilities for the Fund Raiser must be divided up and shared among all committee members equally.
 - d. Minutes for each meeting must be maintained and sent to the QA Department. Minutes shall include each member's participation and responsibilities.
 - e. Minutes will be distributed to all committee members for follow up action as well as to the appropriate Regional Directors.
 - f. Minutes may be shared at Management Trainings, Staff Trainings, Staff Council, and Annual Quality Assurance meetings. All members of the committee will have equal input.
 - g. Accurate financial records will be maintained for accounting purposes. All expenses and income will be accurately documented and checked by more than one committee member and logged on a ledger and documentation reviewed by the Director of Business.

4. At the conclusion of the Fund Raiser, the designated lead must submit all monetary donations or fundraising funds to the Finance Department along with a full accounting and ledger of money spent and received. Final totals are reported to Director of Business and Steering/Executive Director.
5. Funds must be turned in to the Finance Department for deposit as needed if the Fund Raisings is to last multiple days.
6. A Finance Department employee will count the funds with the designated lead and reconcile with the ledger turned in.
7. The Finance Department will prepare and send funds and the ledger to LADD's Financial Institution for tracking and auditing purposes. Funds that have been collected with special instructions per the donor such as designation for use by one specific program will be identified on the ledger. If no specific programs are identified donations will be put into the company wide Fund-Raising Account.
8. When funds are requested for use from the Fund-Raising Account proper receipts must support the use of those funds and are to be turned into the Financial Company for reconciliation.



LADD

WE MAKE THE DIFFERENCE



GOOD MORAL CHARACTER POLICY

PURPOSE

To ensure that LADD employees meet the criteria for good moral character.

SCOPE

This policy applies to all LADD employees and volunteers.

POLICY

LADD will make every attempt to ensure that employees and volunteers for all programs are of good moral character by using the following procedure/standards.

STANDARDS AND DEFINITIONS

Good Moral Character - "Good moral character" means that term as defined in and determined under 1974 PA 381, MCL 338.41 to 338.47. It refers to a personal history of honesty, fairness, and respect for the rights of others and for state and federal law.

PROCEDURE

1. At the time of application all potential employees / volunteers will sign a Release of Information.
2. The Human Resources Department will at a minimum check two references, more as needed.
3. After the Conditional Job Offer has been signed by the potential employee, the Human Resource Department will complete a Drug Screening and Criminal History Background Check that meets contract requirements; these may include the DHHS Child Abuse Registry, CHAMPS, OIG, SAMs, FBI fingerprinting , Motor Vehicle Report, ICHAT, etc.
4. If there is a criminal record and the potential employee indicated "no" on their application and/or the Denial of Existence of Criminal History the person will not be retained due failure to demonstrate honesty and integrity.
5. If potential employee has any adverse records that were correctly reflected on the application, the Director of Human Resources will review the charges and or citations along with references to determine good moral character and suitability for the position.
6. At any time during the application process if unsatisfactory information is discovered then the Conditional Job Offer may be withdrawn in compliance with Fair Credit Reporting Act (FCRA). The Human Resources Department must discuss this information with the Executive Director if warranted prior to taking action.
7. All employees must continuously maintain Good Moral Character to remain employed. Therefore, all employees must report any criminal activity (arrests), convictions, pending convictions and/or changes in Driver's License status as outlined in their Employee Code of Conduct Handbook.
8. Criminal history reviews are completed annually or upon notification of the potential for an adverse finding on the criminal history check. If any adverse findings, then the following must occur:
 - a. Administration will review the record along with the individual's personnel file/history and a separation consideration as to the continued employment of the employee will be made to the Executive Director. Each case will be handled on an individual basis to insure compliance with contracting requirements. The Michigan Workforce Background Check Legal Guide and the MSA 14-40 will be used as guidance for best practice.
 - b. Administration may ask the employee for additional documentation to establish conformity with the Good Moral Character definition. Such documentation could include; court documentation related to the illegal act, additional letters of reference assuring Good Moral Character, a statement from the employee detailing the incident, a statement obtained by Administration by stakeholders who have first-hand knowledge of the employees work history/relationship with the people served, information regarding success of rehabilitation and

personal letter from the employee detailing their rehabilitation. The Executive Director will review the additional material.

9. If it is determined that the employee no longer meets Good Moral Character, then the employee will be separated from employment following the company policy on separations.



LADD

WE MAKE THE DIFFERENCE



HARRASSMENT AND WORKPLACE VIOLENCE POLICY

ZERO TOLERANCE

PURPOSE

To establish the company's position of zero tolerance for any type of harassment or violence by employees. All employees are required to follow the company's Mission, Vision and Values, which embrace treating all people with dignity and respect and aligning your behavior with positive language and actions towards others.

SCOPE

This policy applies to employees at all locations. This policy applies to non-employees who are providing a service or visiting programs where employees are engaged in services. (vendors, contractors, other agency personnel, trades people, etc.).

POLICY

LADD has Zero Tolerance for any type of harassment or violence (verbal or physical) including sexual, racial, disability, religious, ethnic background, age, sexual orientation, gender expression, protected activity, etc. Any type of harassment or violence goes against our Mission, Vision, and Values and it is contrary to basic standards of conduct between individuals. It is prohibited by EEOC, State of Michigan and LADD regulations. Harassment and Violence are contrary to basic standards of conduct between individuals and is prohibited by Equal Employment Opportunity Commission and State/Federal regulations.

Harassment or Violence of any kind will therefore constitute a violation of LADD policy for an employee to engage in any violence, harassing or intimidating act including but not limited to those behaviors defined below. Any such misconduct will subject the employee to corrective actions up to and including immediate separation from employment.

Employees who feel they have been violated or discriminated against in the workplace on the basis of any of the below harassment or violence examples or in any other manner harassed, should immediately report such incidents, following the procedure described below, without fear of reprisal. Confidentiality will be maintained to the extent permitted by the circumstances.

DEFINITIONS AND STANDARDS

It is a standard here at LADD that Harassment or Violence of an employee by any employee or non-employees who are providing a service or visiting programs will not be tolerated. Although the company cannot control people's behaviors, it can control who is employed as well as who we do business with.

Because of LADD's strong disapproval of offensive or inappropriate Harassment or Violent type behavior at work, all employees must avoid any action or conduct which could be viewed as Harassment or Violence of any kind to remain employed.

All employees are required to follow our LADD Mission, Vision and Values that provides positive boundaries for our employees and all stakeholders.

Employees are who create the company's culture. Stopping Harassment and Violence requires creating a culture or an environment where bothersome and unprofessional behavior is not acceptable and creating a positive environment to work and live. This can be done by reminding everyone of the need to follow the **Mission, Vision and Values of valuing P.E.O.P.L.E.** and working together to **MAKE THE DIFFERENCE**; a positive difference in people's lives!

Definitions:

1. **Employee.** Any employee of LADD including PCTs, Managers, Supervisors and Directors or any other employee.
2. **Non-Employee.** Any person who is being paid by LADD for services such as contractors, vendors, or any outside agency employees delivering services such as Community Mental Health, State, Federal, Insurance employees. Also included is any persons LADD employees have to be in contact with while on the job such as a guardian, community member, etc. NOTE: Although LADD has no authority over **Non-Employees**; we will support our employees in reporting to authorities so appropriate action is taken against any discriminatory or violent behavior.
3. **Harassment** is defined as unwelcome physical or verbal behavior such as offensive jokes, belittling comments, slurs, epithets, name calling, physical threats or assaults, ridicule or mockery, insults, offensive objects or pictures, or other interference with work performance that creates an intimidating or hostile work environment. Harassment can also include sexual harassment such as unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature.
4. **Violence** is the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation. It could be language, gestures, or actions that may be considered a threat, in which such conduct interferes with an employee's work performance or creates an intimidating, hostile or offensive working environment.

TYPES OF HARASSMENT

Discriminatory Harassment

➤ **Racial or Ethnic Harassment**

A victim may experience racial or ethnic harassment because of their race, skin color, ancestry, origin country or citizenship.

Even perceived attributes of a certain ethnicity (curly hair, accents, customs, beliefs or clothing) may be the cause; harassment often looks like:

- Racial slurs
- Racial insults
- Racial jokes
- Degrading comments
- Disgust
- Intolerance of differences

➤ **Gender Harassment**

Gender-based harassment is discriminatory behavior towards a person based on their gender or gender expression. Negative gender stereotypes about how men and women should or do act are often the center of the harassment.

Some examples are:

- A male person faces harassment for having what is perceived as a woman's job
- A female person faces harassment based on not 'looking feminine'
- A person chooses not to identify with any gender specific ideology

➤ **Religious Harassment**

Religious harassment is often interconnected with racial harassment, but narrows in specifically on the victim's religious beliefs.

An individual with a religion that differs from the "norm"; may face harassment or intolerance in a variety of ways:

- Intolerance toward religious holidays
- Intolerance toward religious traditions
- Intolerance toward religious customs
- Cruel religious jokes
- Degrading stereotypical comments

- Pressures to convert religions

IMPORTANT NOTE:

LADD celebrates and values the diversity of its community and aims to create a harmonious working and learning environment where the cultural, religious and non-religious beliefs of all members of the LADD are respected. LADD recognizes the right to freedom of thought, conscience and religion, but the right to manifest beliefs is qualified by the need to protect the rights and freedoms of others. We want an environment that ensures equal treatment for everyone, of any religion or none. It is based on the principle that people have the right to their own belief system; however, they have no right to impose their views on others. One of our core values that all employees must follow includes **'appreciating all differences and treating all people with dignity and respect'!**

➤ **Disability-Based Harassment**

Disability-based harassment is a type of workplace harassment directed towards individuals who either:

- Suffer from a disability themselves
- Are acquainted with a disabled person or people
- Use disability services (sick leave or workers' comp)

A person with a disability may experience harassment in the form of harmful teasing, patronizing comments, refusals to reasonably accommodate or isolation.

➤ **Sexual Orientation-Based Harassment**

Sexual orientation-based harassment can be towards people of any sexual orientation (heterosexual, homosexual, bisexual, asexual, transgender, etc.) being different from those around them. Examples may be:

- A homosexual man may face harassment on a construction site whereas a heterosexual man may be teased for working in a salon.
- A person may choose to act in a way that does not align with what some perceive as the 'norm' for their sexual orientation.

➤ **Age-Based Harassment**

Workers 40 years and older are specifically protected by the Civil Rights Act of 1964 in an attempt to promote employment of older people and reduce age-based harassment.

A person facing age-based harassment might be:

- Teased and insulted,
- Left out of activities or meetings, or
- Unfairly criticize for being slow

Simply because of their age and the stereotypes that come with it. Unfortunately, this harassment is sometimes an attempt to wrongfully push the individual into early retirement.

Physical Harassment or Violence

Physical harassment, also often called workplace violence, refers to a type of workplace harassment that involves physical attacks or threats (verbal and/or physical). In extreme cases, physical harassment may be classified as assault.

Physical gestures such as playful shoving can blur the line between appropriate or not, since it's the person on the receiving end who decides whether the behavior makes them uncomfortable.

In order to more clearly define that line, physical harassment should be taken very seriously in the workplace and could end up with legal ramifications such as prosecution besides loss of job.

Examples of Physical Harassment:

Common behaviors include:

- Direct threats of intent to inflict harm
- Physical attacks (hitting, shoving, kicking)

- Threatening behavior (shaking fists angrily)
- Destroying property to intimidate

Psychological Harassment

Psychological harassment has a negative impact on a person's psychological well-being.

Victims of psychological harassment often feel put down and belittled on a personal level, a professional level or both. The damage to a victim's psychological well-being often creates a domino effect, affecting their physical health, social life and work life.

Examples of Psychological Harassment:

Psychological harassment in the workplace might look like:

- Isolating or denying the victim's presence
- Belittling or trivializing the victim's thoughts
- Discrediting or spreading rumors about the victim
- Opposing or challenging everything the victim says

Cyberbullying

Cyberbullying can occur over the internet where communication is not in person; bullying can occur by harmful words and/or emoji gesturing, pictures, etc. Social Media and Instant messaging applications such as Twitter, Facebook, Instagram, Snapchat, and Tik Tok offer opportunities for cyberbullying.

Examples of Online Harassment:

- Share humiliating things about the victim by mass email, text, or mass chat
- Spread lies or gossip about the victim on social media
- Send harassing instant messages or text messages directly to the victim

Cyberbullying Laws - Federal law doesn't explicitly cover "cyberbullying" yet (particularly for adults).

However, the Department of Justice has noted that legal action is possible by prosecuting the online misbehavior under another law.

Sexual Harassment

Sexual harassment is harassment that is sexual in nature and generally includes unwelcome sexual advances or visual, verbal or physical conduct of a sexual nature. This definition encompasses many forms of offensive behavior, including gender-based harassment of a person of the same sex or the opposite sex as the harasser, conduct of a sexual nature that creates an offensive, intimidating or hostile work environment; and coerced sexual conduct by a person in a position of authority in the workplace.

Examples of sexual harassment include:

- Unwelcome sexual flirtation or advances.
- Offering employment, promotions or other benefits in exchange for sexual favors.
- Making or threatening reprisals for refusing sexual advances.
- Visual conduct such as leering; making sexual gestures; displaying sexually suggestive objects or pictures; cartoons or posters; suggestive or obscene letters, notes or invitations.
- Sharing sexual photos (pornography)
- Posting sexual posters
- Sexual comments, jokes, questions
- Inappropriate sexual touching
- Inappropriate sexual gestures
- Invading personal space in a sexual way

Stalking – a form of Harassment - Stalking, defined by the National Institute of Justice as “a course of conduct directed at a specific person that involves repeated (two or more occasions) visual or physical proximity,

nonconsensual communication, or verbal, written, or implied threats, or a combination thereof, that would cause a reasonable person fear” is disruptive to employee’s lives and that can include their time at work.

Examples of Workplace Stalking may be:

- An employee may be stalked by someone they know outside of work whose stalking behaviors creep into their work life. This can include showing up to the victim’s workplace, sending unwanted parcels to work, or calling them at work.
- An employee may become the victim of stalking from a coworker.

Verbal Harassment

Verbal harassment can be the result of personality conflicts in the workplace that have escalated.

Unlike discriminatory types of harassment (such as sexual), verbal abuse is often not illegal. Instead, verbal harassment can be someone who’s consistently mean or unpleasant. Verbal harassment can be particularly damaging since it goes unnoticed and unresolved. Again, here at LADD, remember that ALL employees are required to follow our Mission, Vision and Values of valuing P.E.O.P.L.E. so use this to guide you to remind someone that it must be followed. Always report if it goes uncorrected. Management must be able to communicate with employee’s normal workplace practices throughout the course of employment.

Examples of Verbal Harassment:

Obvious verbal harassment behaviors include things like threatening, yelling, insulting or cursing at a victim in public or in private.

The intensity of any kind of harassment depends upon several factors, some of which are:

1. The degree of unsolicited verbal or physical contact;
2. Repeated actions after complaints or warnings;
3. Physically threatening statements or actions.

ALWAYS REPORT so that the issue can be corrected and all employees are kept safe!

IMPORTANT NOTE: LADD does not tolerate retaliation of any kind. Employees need to report without any retaliation. Please review the Whistleblowers Policy.

1. Complaints of harassment or violence of any type will be handled through the company's **Complaint Reporting Policy** found in the Compliance and Ethics Program.

Additional Guidance:

- If someone is indulging in bothersome or unprofessional behavior you need to immediately remind them of our Mission, Vision and Values that all employees are required to follow at all times. Also let them know exactly where their behavior is stepping out of boundaries. Understand that each of us comes from a different environment and/or culture. A person’s behavior may be defined by what was learned at home, during personal time or have been defined in their childhood. Expressing your concern to them helps not only you, but also them, define what acceptable behavior is. Regardless, all employees are required to follow our LADD Mission, Vision and Values that provides positive boundaries for our employees and all stakeholders.
- Stopping harassment and violence requires creating an environment where bothersome and unprofessional behavior is not acceptable and creating a positive environment to work and live. This can be done by reminding everyone of the need to follow the Mission, Vision and Values of valuing P.E.O.P.L.E. and working together to MAKE THE DIFFERENCE; a positive difference in people’s lives.
- Each of us need to define our boundaries. Always use your voice and tell the person to **STOP**.
- Any type of harassment is unacceptable conduct, and timely corrective action will be taken by LADD when problems of this type exist.
- All employees should feel safe at work. If harassment is occurring, it needs to be reported immediately or at least preferably within 10 days of the alleged occurrence. Reports can be made without fear of negative

consequence for the reporting employee based on the issuing of a complaint. We all need to work together to correct problems and insure everyone is following our Mission, Vision and Values.

2. If it is believed that an employee has engaged in an act of violence or is likely to engage in an act of violence, this must be reported immediately without delay to Management and the Corporate Compliance Officer so that employees are kept safe!
3. Employment will not continue for any employees found to be maliciously harassing and/or engaged in violence as well as possible prosecution to the full extent of the law.



LADD

WE MAKE THE DIFFERENCE



CORPORATE STANDARDS OF CONDUCT

LADD is a high quality community resource for all stakeholders that is dedicated to being an outstanding community partner. The organization will always hold itself to the highest ethical principles, respect all people and remain committed to creating a corporate culture of personal responsibility and ethical business practices.

At LADD we will promote a positive public image that aligns with our mission, vision and values of the company. Company activities will be transparent and conducted in a manner that promotes the principles of inclusion, diversity, human rights and opportunities for all; ensuring the community is better place because LADD is a part of it.



LADD

WE MAKE THE DIFFERENCE



CORPORATE RESPONSIBILITY POLICY

PURPOSE

LADD is a high-quality community resource, for all people; that will always guarantee ethical principles are met, respect for all people is given and a commitment to creating a corporate culture of personal responsibility and ethical business practices is maintained.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to promote a positive public image that aligns with the mission, vision and values of the company. Company activities will be transparent and conducted in a manner that promotes the principles of inclusion, diversity, human rights and opportunities for all; ensuring the community is better place because LADD is a part of it.

STANDARDS AND DEFINITIONS

- Ensure all stakeholders, including employees understand the requirement to immediately report to the CCO, any suspicion of fraud, waste, or abuse in connection with the business of LADD.
- Ensure all employees are responsible to follow the organization's Mission, Vision, and Values and are trained in this area.
- Ensure that all employees are motivated and involved in the continuous improvement of the organization.
 - Value the training needs of all personnel and prepare an annual training program that includes issues of Corporate Social Responsibility in the training sessions.
 - Provide training to new employees on the commitments to Corporate Responsibility.
- Educate and demonstrate to the community the organization's Mission, Vision, and Values while providing services.
- Promote the use of natural supports from the community for persons receiving services.
- Identify, expand and diversify services that are needed in the community.
- Provide opportunities for community inclusion and integration for the people we support and others.
- Assert Human Rights and Values and to be aware of cultural differences and develop systems and procedures that ensure the promotion, protection, interpretation and application of human rights are interpreted the same across different cultural, ethnic and religious traditions.
 - Human rights are the natural-born rights for every human being, universally. They are not privileges.
 - Encourage inclusiveness and diversity.
 - Provide training in cultural diversity including human rights, moral responsibility, discrimination and standards of conduct and
 - Ensure employment of disabled personnel.
 - Guarantee coherence, equal opportunities and no discrimination.
- Ensure basic health, safety and accident prevention measures are taken.



CORPORATE GIVING POLICY

PURPOSE

In an effort to respond to the needs of our stakeholders and promote a positive public image that aligns with our Mission, Vision and Values; LADD has established a process for the review and approval of requests for funds, gifts and/or donations that will benefit the greater community.

SCOPE

This policy applies to all LADD employees, people supported and stakeholders.

POLICY

It is the policy of LADD to engage in Corporate Giving that creates opportunities to advocate for the people supported, educate the public regarding LADD and demonstrates our commitment to good community relations. Due to limited resources decisions will be made that have the potential for the greatest impact and will be on a first come, first served basis.

STANDARDS AND DEFINITIONS

Unless a deviation has been documented as approved by the Executive Director or their designee a single donation is limited to a maximum of \$275.00.

PROCEDURE

1. Stakeholders can contact a member of Management to request or ask for assistance in completing a request for a corporate donation.
2. The Stakeholder, if needed, with Management assistance, will submit the Request for a Corporate Assistance/Donation form along with any other available information to the Director of Business.
3. The Director of Business will review and confirm the information contained in the Request for Corporate Assistance-Donation form and submit the information to the Executive Director or their designee for approval.
4. Following a decision by the Executive Director or their designee, the Director of Business will communicate the decision to the person making the request and document accordingly.
5. If the decision has been made to donate, the Director of Business will coordinate the donation and maintain documentation.

LADD
WE MAKE THE DIFFERENCE



REQUEST FOR CORPORATE ASSISTANCE/DONATION

Stakeholder Name: _____

Stakeholder's Telephone Number: _____

Stakeholder's Email Address: _____

Date of Event: _____

Describe the Event: (include how this applies to the LADD M,V,V or provides an opportunity to advocate for the people or educate the community)

What assistance is being requested: _____

I have requested a donation/assistance per the LADD's Corporate Giving Policy. I understand a request does not guarantee that I will receive a donation/assistance and decisions are made based on making the greatest impact with limited resources.

Signature of Stakeholder

Date

Director of Business

Date

Executive Director

Date

WE MAKE THE DIFFERENCE

Instructions for dispersing funds: _____



GIFTS, BEQUESTS AND DONATION POLICY

PURPOSE

LADD provides supports to vulnerable people; and therefore, must ensure at all times that care is never influenced or could appear to be influenced by gifts, money or favors. It must be made clear that LADD decisions are made solely for the benefit of the people supported. Therefore, LADD has established standards governing gifts, bequests, and donations to all employees.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to promote a positive public image that aligns with the mission, vision and values of the company. All activities will be transparent and conducted in a manner that is free of perceived, potential or actual conflicts or ethical violations. All gifts, bequests and donations will be reported so that proper approval, tracking and distribution will occur.

STANDARDS AND DEFINITIONS

Compensation (of any type) to employees is only made from LADD employer to employee. Therefore, to avoid any appearance of undue influence, protect the integrity of our employees and ensure unbiased care of the people we support, employees are responsible to direct anyone wanting to give a gift to the Corporate Compliance Officer using contact information available at the LADD website.

Gifts, Bequests and Donations are a free contribution to a charitable or public cause, i.e., money material items or services whether delivered all at once or in a series of deliveries.

All gifts, bequests, and donations (referred to collectively as donations) shall be used in strict compliance with the terms stipulated by the donor.

Official acknowledgment of donations will be made through the Business Department and accompanied by an appropriate reference for which the donor may use for tax purposes. If information is available, LADD will send a Thank You Note to the person or company who made the donation.

All monetary donations must be made out to LADD and submitted to the Finance Department following the procedure below. Members of Management are not to accept any donations made out directly to the employee or in the form of cash or gift cards.

Special donation of Flex Time from one employee to another or company to employee - If an employee makes the decision to donate available flex time to another employee due to a hardship by that employee the Director of Human Resources will coordinate with the Regional Director to review and document the request and approval. The Director of Human Resources will coordinate to ensure documentation is kept in the personnel file of each employee and that time keeping and payroll are appropriately adjusted. The Steering Committee or Executive Director must approve employer to employee.

Some exceptions exist such as:

- Food gifts, baskets, cookies, candy and such gifts can be shared at any given location if all employees have equal access.
- Gifts such as t-shirts, pens, trade show bags and all other trinkets that employees obtain, as members of the public, at events such as conferences, training events, seminars, and trade shows, that are offered equally to all members of the public attending the event.

- Attendance, food and beverages at events, exhibitor trade show floor locations, press events, and parties funded by conference or event sponsors.
- Cards, thank you notes, certificates, or other written forms of thanks and recognition.

***Under certain conditions and with approval by the Executive Director or their designee a deviation from these standards may be granted upon specific donor requests. Documentation must be completed by the Corporate Compliance Officer noting the request. ***

PROCEDURES

1. When possible, prior approval for all donations must be obtained by a member of Management. If this is not possible due to the timing of the donation, approval must be obtained as soon as possible after receipt by a member of Management.
2. Following approval, donations such as merchandise, goods, services or items of value must be reported to the Finance Department. The Finance Department will log the item on the Donation Ledger noting the item donated, date of donation, the donor's name along with address of donor, value, any special instructions and if applicable who the donation is for, must all be documented.
3. The Finance Department will notify LADD's Financial Institution of the donation, providing details noted in #2 above.
4. When necessary, the member of Management responsible for receiving the donation will coordinate with the Director of Business to secure or store the item/s donated.
5. Following approval, all monetary donations must be submitted to the Finance Department unless special approval by the Executive Director or their designee has been obtained. Monetary donations must be reported to the Finance Department regardless of whether special approval for dispersing was obtained.
6. The Finance Department employee will count down the funds with the member of Management responsible for receiving the donation.
7. The Finance Department will log the monetary donation on the Donation Ledger noting the amount donated, date of donation, the donor's name along with address of donor, any special instructions and if applicable who the donation is for must all be documented.
8. The Finance Department will prepare and send funds to LADD's Financial Institution for tracking and auditing purposes. Funds that have been collected with special instructions per the donor such as designation for use by one specific program will be identified for LADD's Financial Company. All funds will be put into the company Fund-Raising Account.
9. Monetary donations that are designated for specific programs/activities must be tracked by Management and then all receipts from these expenditures need to be turned back into LADD's Financial Institution to support the use of the funds. (i.e. A family donates \$200.00 to have a pizza party, the program must turn back in \$200.00 worth of receipts to support use of the donation).

WE MAKE THE DIFFERENCE



TRADEMARK/LOGO USE POLICY

PURPOSE

The purpose of the LADD Trademark/Logo Use Policy is to describe the logo in clear terms, define general classes of acceptable and prohibited use. The policy does not define every imaginable use of the logo, but does provide a clear path to seek approval for variations of the standard logo.

SCOPE

This policy applies to all LADD employees.

POLICY

It is the policy of LADD to ensure the LADD logo is maintained, as designed and with the original intention to be used so that a consistent public image is presented in all official LADD endeavors.

STANDARDS AND DEFINITIONS

- The LADD logo cannot be modified, used in an inappropriate manner or altered/used for reasons other than official LADD business without the express written permission of LADD Administration. This includes the use of altered logo on letterhead, clothing, websites, promotional materials or any other items.
- This LADD logo will help to strengthen the LADD name and image through a consistent branding, a distinctive logo used throughout all of our events, publications, and activities.
- The basic LADD logo consists of two parts: the graphic element and the text element. There are variations that add the company address and full name.



- Proper use of the logo will incorporate both the graphic and text elements. It is understood, however, that certain uses of the logo preclude the inclusion of the text element. For example, use of the logo on a pin or badge, or on the spine of a book may necessitate the use of the graphic element alone. Wherever possible, however, the graphic and text elements should be used together.

PROCEDURE

Committees and projects of the LADD organization are free to use the LADD logo, provided the following guidelines are considered:

1. The logo and text should be used together, as defined, whenever possible.
2. The typeface shall not be altered or replaced with another.
3. The proportions of logo and text shall be retained when possible. It is understood that certain design opportunities necessitate the use of the logo without the text.
4. Decoration of the logo is acceptable as long as the basic logo remains clearly visible.
5. If a design is to include the LADD logo then the design must to be submitted to Administration for written approval prior to printing.
6. If requesting the LADD logo to be used on a clothing item, then approval must be obtained.

7. For clothing items, the left chest is always only used for LADD logo although the LADD logo can be in other areas.
8. The people who receive support services from LADD, can have shirts that have positive sayings on them, but not the LADD logo. This is, due to the fact this may draw unnecessary attention or stigma to them.

Prohibited Uses

Examples of prohibited use include, but are not limited to, the following:

1. Personal use of the LADD logo in social networking sites such as Facebook, LinkedIn etc.
2. Any implication of endorsement by the organization or its activities;
3. Commercial uses (placement of the logo on product packaging);
4. An individual's use of the logo for purposes other than acknowledging membership or participation in our activities;
5. Combination of the organization's logo with another logo unless it is part of a list of donators, etc.
6. Violations of this policy must be reported to a member of management for further action.





AUDITING AND MONITORING POLICY

PURPOSE

To establish the company's position on Auditing and Monitoring. The purpose of Auditing and Monitoring system is to have a comprehensive approach designed to include different departments and levels of management to create checks and balances for ensuring compliance, evaluating processes and improving the effectiveness of systems through the use of structured data collection, management and outcome reporting.

SCOPE

This policy applies to all LADD management, and may involve employees and people supported. Managers, Supervisors and Quality Assurance/Compliance members are responsible for conducting audits. Other members of management may conduct audits if necessary. Please see the Annual Audit list below along with the responsible person.

POLICY

It is the policy of LADD to promote a positive public image that aligns with the Mission, Vision and Values of the company. All services and locations will be reviewed to ensure compliance with applicable laws, contractual requirements, organizational standards, systems and practices. Should non-compliance occur, immediate action will be taken to correct the non-compliance through the quality improvement process, correcting the clinical record and when necessary repayment of funds and necessary contacts to meet applicable federal/state laws and contracts.

STANDARDS AND DEFINITIONS

Services Department

- Services will complete designated audit worksheets according to the schedule outlined.
- Services will complete timely corrective action that remedies noncompliance.

Compliance Department

- Compliance is responsible for the development of audit worksheets and auditing schedules in conjunction with the Services Department to achieve service and program compliance. All audit worksheets and the audit schedule are located in the R: Drive \010 Auditing and Monitoring.
- The Compliance Department will complete an annual audit schedule and provide to the team.
- Compliance is responsible for completion of data tracking and reports so that corrective action, including training and system change, in conjunction with Services and Quality Improvement Departments, occurs. All audit reports are located in the O Drive:\Company Reports.
- Compliance will review data, observe physical locations and provide recommendations for improvement to Steering Committee
- At the end of the audit cycle (January through December) the Compliance Department will remove all audit worksheets and reports and save in a folder by year. The Compliance Department will then set up new folders to begin the new audit cycle.

Corporate Compliance Officer

- The Corporate Compliance Officer (CCO) is responsible for oversight of the auditing and monitoring process.
- In the event an audit reveals potential violations, trends or areas for improvement, the CCO will take appropriate action including:
 - Conduct investigations
 - Coordinate with Human Resources and Service regarding corrective action
 - Coordinate with Quality Improvement regarding system change, training and modification to policies and procedures
- The results of all audit and monitoring functions are provided to the CCO, who will report results to the Steering Committee and Executive Director on a regular basis, no less than annually.
- The CCO will direct implementation of Steering Committee and Executive Director recommendations.

The CCO reports directly to the Executive Director for any critical compliance issues.

Steering Committee

- The Steering Committee will review audit results and trends documenting recommendations in the Steering Committee meeting minutes.
- The Steering Committee will determine high risk areas for focused audits annually during Strategic Planning.
- The Steering Committee will direct the Emergency Management Committee to coordinate with Quality Assurance to address areas of risk and related audit findings.

Auditing Standards

Audit Type	Audit Name	Audit Worksheet Location	Person Responsible	Audit Schedule <i>Compliance to complete schedule</i>
Quarterly Environmental Safety Checklist- To be done by apartment if applicable	Quarterly Environmental Safety Checklist Audit	R:Manager\010 Auditing and Monitoring\Monthly Environmental Safety Checklist Audit	Manager	Quarterly
Persons Medications	Annual Quality Assurance Audit	R:Manager\010 Auditing and Monitoring\Annual Quality Assurance Audit	Supervisor	Annual
Person Administrative				
Program Operations				
Program Maintenance				
Emergency Guide Book and Drills				
General Appearance of Program LICENSED ONLY				
Person Centered Plan 30 Day Post PCP Review	N/A	N/A	Supervisor	According to PCP Dates
CLS specific versions of the above audit types are completed for CLS services		R:Manager\010 Auditing and Monitoring\Audit Worksheets\CLS Audits\“multiple”		
	Individual Service Annual Quality Assurance Audit		Supervisor and/or Regional Director	Annual
Home Help Billing Logs And Occupancy Logs	N/A	N/A	Regional Director	Monthly
Goals/Objectives/Billing Verification	Goals/Objectives/Billing Verification Audit	R:Manager\010 Auditing and Monitoring\Audit Worksheets\ Compliance Audits\“multiple”	Compliance	Annual
Personal Allowance	Personal Allowance Audit		Compliance	Monthly
Medical and Health Conditions	Medical and Health Conditions Audit		Compliance	As needed by IR/RCA
Safety and Physical Plant	Safety and Physical Plant Audit		Compliance	As needed by IR/Barriers-EMC

PROCEDURE

AUDIT PROCESS

1. The responsible person will access the correct audit worksheet, according to the Audit Standards section.
2. All audit worksheets are located in the Manager R Drive, in the folder 010 Auditing and Monitoring in a subfolder called Audit Worksheets.
3. The audit worksheet is scored as follows: 0= NO and 1= YES. Any areas that do not apply are noted as N/A.

Quarterly Environmental Safety Checklist Audit- MANAGERS

1. This audit worksheet is available to be completed electronically or can be printed and completed as a paper copy if needed.
2. The Manager or their designee will complete the audit worksheet.
3. Once the audit worksheet has been completed the Manager will review the audit worksheet:
 - a. If a question has been left blank the Manager must complete the question by scoring it.
 - b. If a question receives a score of 0 the Manager must complete the Corrective Action Plan (CAP) section of the audit worksheet.
 - c. Score the audit worksheet by dividing the total score of all questions added together by the number of questions that were scored. Do not count N/As in the calculation. For example, if the total of all responses to questions is 50 and all 52 questions were scored, with no N/As the scoring is $50/52=.96$ or 96%. If the total of all responses is 45 and there are 7 questions marked with N/As the scoring is $45/45=100\%$.
 - d. The completed and scored audit worksheet will be saved into the system as noted below by the 5th of the month following the month completed i.e. 29 December due by 1/05.
4. Once the audit worksheet is scored by the Manager the Manager will:
 - a. For audit worksheets completed electronically, save the document in R:\010 Auditing and Monitoring\02 Completed QES Checklist Audits (M). The document will be named the program number and the month it was completed for i.e. 29 December.
 - b. For audit worksheets completed as paper, scan the document and save in R:\010 Auditing and Monitoring\02 Completed QES Checklist Audits (M). The document will be called the program number and the month it was completed for i.e. 29 December.

Special Note

For audits that have been completed in paper form and corrections are required. Each time corrections and additions are made to the document it must be saved in place of the original document so the most up to date document is in the folder. If the corrections are completed on the electronic version, simply save the updated document in place of the original. **Regardless of corrective action original scores and percentages are NEVER changed.**

5. On a monthly basis the Supervisor:
 - a. Will review the completed audit worksheet to ensure corrective action is being completed as noted.
 - b. Validate the percentage score is accurate.
 - c. Enter the percentage score in the correct location on the Quarterly Environmental Safety Checklist Report located in O:\Company Reports\All QA Audit Reports\00 Quarterly QES Checklist Audit (REPORT)(M). Scores are entered in the report by the 15th of the month following the month completed i.e. P29 December due by 1/15.
 - d. Additional comments are to be added to the Report when a percentage score is less than 100%. Comments are to be left by right clicking on the QES Score cell. After right clicking, scroll down and select the Insert Comment prompt. A dialogue box will open with your name in it, you can type your comments here.
 - e. Supervisors will monitor areas that have required a CAP and note on the report the date the CAP was completed.
6. On a quarterly basis the Compliance Department will complete a summary report that indicates:
 - a. Any outliers not achieving a score of 100%.
 - b. Any outliers not completing the audit process on a monthly basis.

- c. Company trends regarding CAPs.
- d. All information will be consolidated for review by Dept. Directors on going for improvements and used during Strategic Planning.

Annual Quality Assurance Audit- SUPERVISORS

1. This audit worksheet is available to be completed electronically or can be printed and completed as a paper copy.
2. The Supervisor will complete the audit worksheet according to the schedule provided by the Compliance Department. Modifications to the schedule must be approved by the Regional Director and communicated to the Compliance Department so the schedule is updated.
3. Once the audit worksheet has been completed the Supervisor will review results:
 - a. If a question receives a score of 0 the Supervisor must complete the Corrective Action Plan section of the audit worksheet for each item scoring 0.
 - b. Once completed the audit worksheet is scored by dividing the total score of all questions per section added together by the number of questions that were scored in that section. Do not count N/As in the calculation. For example, if the total of all responses to questions is 50 and all 52 questions were scored, with no N/As the scoring is $50/52=.96$ or 96%. If the total of all responses is 45 and there are 7 questions marked with N/As the scoring is $45/45=100\%$.
4. Once the audit worksheet is scored by the Supervisor the Supervisor will:
 - a. For audit worksheets completed electronically, save the document in the R Drive:\010 Auditing and Monitoring\03 Completed Annual Quality Assurance Audits (S). The document will be named the program letter and number and Annual Quality Assurance Audit i.e. P29 Annual Quality Assurance Audit.
 - b. For audit worksheets completed as paper, scan the document and save the document in the R Drive:\010 Auditing and Monitoring\03 Completed Annual Quality Assurance Audits (S). The document will be named the program number and Annual Quality Assurance Audit i.e. 29 Annual Quality Assurance Audit.

Special Note

For audits that have been completed in paper form and corrections are required. Each time corrections and additions are made to the document it must be saved in place of the original document so the most up to date document is in the folder. If the corrections are completed on the electronic version, simply save the updated document in place of the original. **Regardless of corrective action original scores and percentages are NEVER changed.**

5. On a monthly basis the Regional Director:
 - Will review the completed audit worksheet to ensure corrective action is being completed as noted.
 - a. Validate the percentage scores are accurate.
 - b. Enter the percentage scores in the correct location on the Annual Quality Assurance Audit Report located in O:\Company Reports\All QA Audit Reports\Annual Quality Assurance Audits Report.
 - c. Additional comments are to be added to the Report when a percentage score is less than 100%.
6. On a quarterly basis the Compliance Department will complete a summary report that indicates:
 - a. Any outliers not achieving a score of 100%.
 - b. Any outliers not completing the audit process on a monthly basis.
 - c. Company trends regarding CAPs.
 - d. All information will be consolidated for review during Strategic Planning.

Person Centered Plan 30 Day Post PCP Review- SUPERVISORS

The 30-Day Post PCP Review is completed per the PCP process outlined at O:\01. Management Manual\LADD FORMS & PROCEDURES\PCP and Service Delivery\My PCP Process. SIL. Licensed

Home Help Billing Logs and Occupancy Logs- REGIONAL DIRECTOR

Home help logs and occupancy logs are review for accuracy on a monthly basis prior to claims being submitted for payment. After review and verifying the information is correct the Regional Director signs the document to indicate their approval for the billing process to proceed.

Compliance Audits- COMPLIANCE DEPARTMENT

1. The Compliance Department will complete electronic versions of the **Goals/Objectives/Billing Verification Audit, Medical and Health Conditions Audit, Safety and Physical Plant Audit** worksheets according to the schedule outlined in the Audit Standards section.
 2. Once the audit worksheet has been completed the Compliance Department will:
 - a. Score the audit worksheet by dividing the total score of all questions added together by the number of questions that were scored. N/As will not be included in the calculation. For example, if the total of all responses to questions is 50 and all 52 questions were scored, with no N/As the scoring is $50/52=.96$ or 96%. If the total of all responses is 45 and there are 7 questions marked with N/As the scoring is $45/45=100\%$.
 3. Once the audit worksheet is scored and signed by the Compliance Department the Compliance Department will:
 - a. Save the document in the R Drive:\010 Auditing and Monitoring\04 Completed Compliance Audits (Nan). The document will be named the program number and the type of audit i.e. 29 Goals-Objectives-Billing Verification. All Compliance Department audits are completed in electronic form.
 4. The Compliance Department will enter the percentage score from the completed audit worksheet on the Compliance Audits Report located in the O Drive:\Company Reports\All QA Audit Reports\03 Compliance Audit (REPORT).
 5. For scores of zero the Compliance Department will require a CAP and note on audit reports the date the CAP has been requested.
 6. The Compliance Department will send an email notifying the Manager of the need for a CAP. The Supervisor will be included in the email.
 7. Once the Manager has completed the CAP they will reply to the email notifying the Compliance Department the steps taken to correct and the date corrected. The Supervisor will be included in the email.
 8. Once the Compliance Department has the completed CAP they will note the correction on the original audit worksheet and note the date the CAP was completed on the audit report.
 9. On a monthly basis the Services Team:
 - a. Will review the completed audit worksheets to ensure corrective action is being completed as noted.
 10. On a quarterly basis the Compliance Department will complete a summary report that indicates:
 - a. Any outliers not achieving a score of 100%.
 - b. Company trends regarding CAPs.
 - c. All information will be consolidated for review during Strategic Planning.
-
1. The Compliance Department will complete electronic **Personal Allowance Audits** of all people supported that LADD is Representative Payee for on a monthly basis.
 2. This audit and report are combined into one document. Due to the nature of this audit only a perfect score is acceptable therefore no percentages are calculated.
 3. Once the audit has been completed the Compliance Department will save the results on the Personal Allowance Audit Report located in O:\Company Reports\All QA Audit Reports\Personal Allowance Audit Report.
 4. The Compliance Department will send notice to the Supervisors via email, with a link to the report, notifying them the month of reviews has been completed.
 5. On a monthly basis the Supervisor will review required corrections with the Manager. Together the Manager and Supervisor will complete corrections as follows:
 - a. All Personal Allowance receipts, ledgers bank documents are due by the 10th of the following month, which means that receipts, bank activity and bank withdrawal slips are saved in Citrix

- by the 10th ready to be audited. (For more information please refer to the Personal Allowance Policy).
- b. By the 10th day of the following month, the Personal Allowance Audit report will be completed and saved in the Company Reports folder.
 - c. Indications that corrections are needed are if an item is marked as 0, or there's a comment indicating somethings "needs" done.
 - d. If the comments say: "In the future please", this means that you don't have to go back and fix the item, but need to review that comment and follow those instructions for future. So for example it may say "In the future please scan receipts going in the same direction", so now, you know that next time you scan receipts you are scanning them all in the same direction.
 - e. If the note says "Administrative" that means the manager may need additional training and the supervisor will review.
 - f. Managers will review the Personal Allowance Audit report and make corrections; Supervisors will verify that corrections were completed by the Manager and initial next to the correction.
 - g. Managers will enter in the note's column of the Personal Allowance Audit Report as follows:
 - a. What the corrections were
 - b. Date completed
 - c. Initials
 - h. Do not change the numbers or delete information entered on report by Compliance.
 - i. Corrections are due by the 10th of the following month by the manager or supervisor.
 - j. If you open a report and it says it is "Read Only" that means someone else has the report open. You can review the report, but cannot make changes while in "Read Only". You will need to wait until the other person is done to enter your corrections.
6. On a quarterly basis the Compliance Department will complete a summary report that indicates:
- a. The Compliance Department will continue to follow up until all corrective action has been completed.
 - b. Company trends regarding CAPs.
 - c. All information will be consolidated for review during Strategic Planning.

LADD

WE MAKE THE DIFFERENCE



RESPONDING TO AUDIT FINDINGS FROM EXTERNAL MONITORING AGENCIES

PURPOSE

LADD will respond to audits and findings delineated in reports resulting from auditing by external regulatory agencies in a timely and thorough manner so that corrective action is completed and communicated within the entire organization and to the external regulatory agency.

SCOPE

This policy applies to all LADD support services and employees.

POLICY

It is the policy of the LADD to operate in adherence to federal, state and local regulations or laws pertaining to service provision and funding source.

STANDARDS AND DEFINITIONS

1. The Compliance Department will be notified immediately of the receipt of a notice of audit by an external regulatory agency. The CCO will work with the external regulatory agency to provide the requested information in the timeframe required. All documentation of the audit will be maintained by the CCO.
2. If the audit is part of routine auditing completed annually by Contract Agencies the Services Department will respond to the audit accordingly and document in the audit database.
3. Audit findings that result in recommendations or request for a corrective action plan will be responded to within 5 business days unless a stricter timeline has been required in the findings report.

PROCEDURES

1. Upon receiving an audit report from a regulatory agency, the appropriate LADD Director will review the report and collect information, resources and the appropriate personnel in order to take immediate corrective action and development of a written response that is to be reviewed by the Director of Operations and Development prior to sending to the external regulatory agency.
2. The Director will begin the process of documenting the audit by starting a folder in G:\Administration\Audits.ORR.POC.RCA.Investigations and notifying the Compliance Department.
3. The Director is responsible for assuring the development of a response to each audit finding, by way of a Corrective Action Plan.
4. The Corrective Action Plan will address the following as needed:
 - The individuals affected by the findings.
 - The measures put in place or systematic changes made to ensure that the practice does not recur.
 - Identify who will carry out these measures and who is responsible for completion.
 - Target dates for completion and/or date of completion.
 - How the corrective action(s) will be monitored and who will do the monitoring.
 - Addressing any recommendations given within the report..
5. The Corrective Action Plan will be sent to the external regulatory agency by the stated due date by the Director and file a copy in the correct Administrative file.
6. The Director will be responsible to ensure a thorough review of system changes has occurred and that any changes have been updated or incorporated by the appropriate Department.
7. The Director will be responsible for ensuring system changes resulting from the Corrective Action Plan have been communicated throughout LADD.



COMPLIANCE AND ETHICS TRAINING POLICY

PURPOSE

this policy establishes the framework for employees and Business Associates to receive the appropriate training relative to compliance, ethics and HIPAA and comply with all state, federal and company compliance requirements and policies.

SCOPE

This policy applies to all employees and Business Associates of LADD.

POLICY

It is the policy of LADD to ensure that all employees and business associates receive appropriate training in the Compliance and Ethics Program and their responsibilities to adhere to program policies.

STANDARDS AND DEFINITIONS

The goal of compliance training is to ensure that all LADD employees and Business Associates are aware of the laws, standards and policies so they are able to exhibit effective day-to-day decision-making and actions, ensure consistent application, prevent or limit situations that may put the organization at risk both legally and financially and finally promote positive working relationships.

Compliance and Ethics training will include the following topics:

Deficit Reduction Act (DRA) - The DRA includes several sections that affect entitlement programs and written to increase enforcement for fraud, waste and abuse. There are both State and Federal versions that establish systems for investigating and prosecuting lawbreakers and collecting fines and overpayments. The Medicaid Integrity Program (MIP) is one of those systems.

False Claims Act - The False Claims Act among other things makes it a crime to file a false claim to the government for payment.

Federal Anti-Kickback Statute - The Federal Anti-Kickback Statute prohibits the offer, payment or acceptance of money (or anything of value), directly or indirectly, overtly or covertly in return for referring for a service or purchasing of goods referring an individual to a person for the for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program.

Whistleblowers Protection Act - a law to protect employees by making it so an employer cannot discharge, threaten, or otherwise discriminate against an employee because the employee reports or is about to report a violation of the law.

Health Insurance Portability and Accountability Act (HIPAA) - An act passed by congress requiring national standards for the electronic exchange, privacy and security of health information.

Health Information Technology and Education for Clinical Health Act (HITECH) - An additional act passed to supplement HIPAA standards by establishing increased penalties and enforcement for violations of confidentiality.

Additional content will include an overview of the Compliance and Ethics Program, reasons/benefits of the program, the elements of the program, expected employee behavior/conduct and reporting obligations.

All employees and Business Associates are trained that they must immediately report to the CCO, any suspicion of fraud, waste, or abuse in connection with the business of LADD as well as suspected breach of confidentiality events.

Employees will be trained at time of hire, annually and when entering into a management position. Employees may also receive remedial training as part of the discipline process. Business Associates will be trained per the Business Associate Policy.

PROCEDURE

New Hires

1. All new Employees must attend New Hire Orientation prior to beginning work.
2. When available the CCO or designee will participate in the compliance portion of New Hire Orientation and New Management Training (if applicable).
3. Employees will be given an opportunity to ask questions.
4. Training records will be maintained by the Human Resource Department.

Current Employees

1. All current Employees must complete on-line compliance training on an annual basis. Failure to do so may subject the employee to disciplinary action.
2. Training records will be maintained by the Human Resources Department.
3. As part of the discipline process an employee may be required to complete additional compliance training. Record of the required training will be documented through the investigation process (see Investigation Policy). Proof of completed training will be maintained by the Human Resource Department.
4. All employees entering into a management position will receive additional compliance training with proof of training maintained by the Human Resource Department.
5. Each member of the management team will receive training regarding use and access to the Manager's Manual contains training materials and resources. All materials are arranged to maximize access and ease of use so Management provide training and education to employees. The Management Manual is available in the Remote Desktop.
6. The LADD Directory which contains LADD Policies, the Handbook Code of Conduct, CEP and other valuable resources is available by logging in on the LADD website.
7. Several Quality Assurance documents, Corporate Compliance documents and training materials are available on line for management, employees, people supported/guardians and other stakeholders.
8. Each member of the Management Team receives training on the policies, procedures and expectations of LADD on a routine basis by PPF (Policy, Procedure, Forms) online training and at staff and management meetings.
9. The minutes of all committees are available for review.
10. CARF manuals are available for review by management.
11. Administrative staff will receive ongoing continuing education training in specialty areas and in turn train the Management Team.
12. Additional trainings will be made available to all management staff.
13. Outcome reports will be reviewed by members of management for input on how to improve or maintain quality services.



INVESTIGATION POLICY

PURPOSE

To establish a policy through which complaints are investigated in a fair and consistent manner in support of the Complaint Reporting Policy.

SCOPE

This applies to all employees of LADD.

POLICY

It is the policy of LADD to complete thorough, timely and unbiased investigations of all complaints and suspected wrongdoing.

STANDARDS AND DEFINITIONS:

1. Investigating what appears to be an action or a situation requiring remedial actions may involve the CCO and Department Directors clarifying policies, reviewing, recommending revision and if necessary development of new policy, procedure, forms in order to prevent future occurrences.
2. Behaviors that could require remedial actions might include the following:
 - Failure of an individual to understand and carry out required procedures and policies;
 - Inappropriate or improper implementation of the LADD Compliance and Ethics Program;
 - Not reporting when aware of issues;
 - Negligent or malicious behavior.
3. If remedial action is necessary, the affected individual(s) will be notified of the concerns regarding their performance, and if applicable remedial actions may include:
 - The individual(s) will be required to take part in an educational/training program focused on the problem area and/or
 - The individual(s) may be reassigned, suspended with or without pay, demoted, transferred or subject to other disciplinary action up to and including separation from employment.
 - An employee will be subject to disciplinary action if LADD concludes that the employee knowingly fabricated, exaggerated, or minimized a report of wrongdoing either to injure someone else or to protect him/herself or others.
 - An employee whose report contains admissions of personal wrongdoing will not and cannot be guaranteed protection from discipline. LADD generally will give positive weight to self-confession in determining disciplinary action but the extent depends on factors such as whether the employee's conduct was previously known to LADD, whether discovery of the conduct was imminent, and whether the confession was complete and truthful and whether the conduct violated people's rights or agency contracts or other regulations.

PROCEDURE

1. Upon receiving a report of suspected wrongdoing, improper behavior or violation of company policy and procedure the CCO will immediately begin the investigation process by documenting the details of the report and organizing the investigation.
2. The CCO will begin the investigation by documenting an investigative action plan that may include the following:
 - a. Date
 - b. Person reporting
 - c. Description of the incident
 - d. Develop list of questions to help determine the validity of the report

- e. Develop a list of individuals to be interviewed
 - f. Identify gaps, additional risks
 - g. Identify additional, supporting pieces of information
 - h. Develop recommendations and contingencies
3. Upon completion of the investigative action plan the CCO will coordinate with other Directors to formulate the next steps of the investigation which may include delegating portions of the investigation to others to complete interviews and research of applicable laws, regulations, contract standards or policies and procedures.
 4. The CCO will document and/or collect documentation to support the investigation.
 5. The CCO will report findings to the Executive Director or their designee and/or Compliance Committee/Steering Committee who may seek legal counsel for guidance and corrective action steps.
 6. The CCO will be responsible for making sure follow up has taken place and may consist of discipline, additional training and reporting to authorities.
 7. The CCO, when possible will report to the original complainant regarding findings.
 8. The CCO will insure immediate action is taken to implement corrective action and coordinate with the Services and QA teams to implement system changes to reduce/eliminate the possibility of future reports.
 9. When applicable full disclosure will be made to the correct governmental or legal authority. A Notice of Findings of the investigation, findings and corrective action will be included as required.
 10. The CCO will maintain investigation documentation, track data for trend analysis and report annually as part of the Strategic Planning process.
 11. The Executive Director or their designee may require additional investigation from a third party under certain circumstances, if warranted to insure objectivity.



LADD

WE MAKE THE DIFFERENCE



BILLING, PAYMENT AND PERSONAL FUNDS BENEFIT RECONCILIATION PROCEDURE – OFFICE USE

PROCESS FOR FUNDS RECEIVED- LADD use of Remote Deposit Capture Machine

1. The incoming mail is to be opened by a member of the HR Department. At the time the mail is opened all checks will be entered on the pre-cash list by the HR Department employee.
2. Checks will be deposited by Finance Specialist weekly using the remote deposit capture machine as follows:
 - a. On the Huntington Bank website go to Receivables then Remote Deposit Capture
 - b. Click on Capture Deposits to left of screen
 - c. Then under Locations click on **Check & Remit Payments** for any check coming in with a check stub (Skirt) or click on **LADD** for when we have only a check with no Stub.
 - d. Then Click on Account and choose either **Client Benefits** or **General Account** depending on what check you are scanning.
 - e. Fill in the amount of the total checks you are going to be scanning in. You must put the total to move on.
 - f. Then Click on **Create Deposit**
 - g. It will take you to a screen where you can then click on **Scanning** in the bottom lower corner then all checks and stubs will be scanned into the system.
 - h. The scanner reads the stubs and check and the total amount of the checks deposited must match the amount of what was typed in on the previous screen (the total # from the Pre- Cash List) all lines must be green if not green must fix each line. (Can re scan a check & stub if necessary)
 - i. May scan up to 100 checks at a time. Once checks are scanned the scanner stamps electronically presented on check.
 - j. Once all transactions/scans are green can then submit **Transmissions**.
 - k. To see previous deposits and download transactions in Huntington, go to **Research**, click on the dates of the Transactions you want to see.
 - l. Click on the Locations and choose accounts. Under Query for Transmissions, click on Deposits in drop down box, - where = posting date- fill in date to box to far right must be full date i.e. 01/31/2018 then click on search
 - m. Highlight the transaction you want to see click on drop down box- **Click on 1 x3** Fronts only and then click on **View PDF**.
 - n. Then save the deposits by date into Remote Desktop Z:\FOI DEPOSITS\DEPOSITS FOI so this can be emailed to FOI with the pre-cash list and for reference for LADD if needed.
3. Once checks are scanned through the remote deposit capture an email will be sent to FOI (along with the pre-cash list and the deposit pictures downloaded from Huntington for that day. Special attention is given to making sure any **NOTES** on the pre-cash list and checks stating how funds need to be distributed will be adhered to. **NOTES** are from Guardians/Payees stating how they want the funds distributed to the person supported and when possible must be honored.
4. Checks received on days when deposits are not done will be locked in the safe until deposit day when they are then logged on the pre-cash list by the Finance Specialist and then deposited into the bank.
5. Once checks have been scanned into the Huntington Bank Remote Capture system checks will be kept in a file folder (in the safe in the LADD office) for 30 days before being destroyed by a member of the Finance Department.

PROCESS FOR FUNDS RECEIVED- LADD cannot use the Remote Deposit Capture Machine

1. There are rare circumstances where checks for personal allowance may come to the office. In most cases these checks are made payable to the person supported and may include the name of a member of management. These checks cannot go through the Remote Deposit Capture Machine because they lack the endorsement to LADD.

- a. Checks that come in as described above will be entered on the checks received ledger kept in the safe in the LADD office.
- b. A copy of the check and the original will be kept in the safe along with the checks received ledger.
- c. The Finance Specialist will communicate with the Manager to make arrangements to pick up the check.
- d. It may be necessary for the Finance Specialist to cash the check for the person because they do not have a bank account to do so.
- e. Regardless of whether the funds are a check or cash it must be picked up by the person supported and/or the manager at the office.
- f. Upon receiving the cash or check the person will sign and date the copy of the check and a member of the Finance Department will sign and date as well. A copy of the signed and dated check will be given to the person and/or manager for their records and a copy will be filed in the person's Administrative file at the office.
- g. The checks received ledger will also be signed accordingly to reflect the transaction.

PROCESSES FOR BILLING SERVICES

Definitions and Standards

Occupancy Logs – (Used for Contract Agency billing for specialized residential locations only) Are due on the 10th of the month. Managers must sign the Occupancy Log to indicate that they have reviewed for accuracy and clarity before submitting the form to their Supervisor. The Supervisor reviews for accuracy and signs before forwarding to the Regional Director for final review.

Billing Logs – (Used for Contract Agency billing for CLS and Respite only) Completed by the CLS Department based on completed documentation that notes the start and stop time for services. These logs are not signed and only initialed after billing the service.

Activity Tracking – (Used for Contract Agency billing for SIL only) Are due on the 10th of the month. Managers enter times when the person leaves and returns to the location. Notes about where the person has gone or who they have met with are included as well.

Billing Worksheets – (Used for Contract Agency billing for SIL only) Are completed by the billers using information from Activity Tracking to assist with claims entry into Contract Agency specific billing sites.

Personal Care Services Provider Log – (Used for Home Help Billing) Are due on the 1st of the month. Managers must sign the Personal Care Service Logs, where it says Provider Signature. Signatures of the people supported are included for some insurers, consult with the Finance Specialist for requirements. The Supervisor reviews for accuracy and ensures the forms have been correctly signed. The Area Supervisor informs the Regional Director the Logs are ready to go to the Finance Specialist. RD notifies the Finance Specialist when to begin processing the billing.

When a person supported begins receiving Home Help for the first time the Manager is to start documenting progress notes on the person supported as soon as the Home Help application has been started. Documentation must consist of the services provided for the person. Starting the documentation process on progress notes at the time of the application will allow LADD to be able to bill for the services provided once the approved Time and Task sheet comes to the person's home, which may take up to 45 days. For additional information refer to R:\002. Electronic Occupancy Logs\Home Help Services.

Marking a Person as Absent – Marking a person as absent is based on individual circumstances and it is recommended questions in this area be directed to your supervisor. These standards apply to both Occupancy Logs and Personal Care Services Provider Logs as follows:

- A person is marked as present for an entire day if they were in the location up to and including 8:00 am. This means they received safety supervision and possibly received a meal, personal care assistance, and medication administration.

- A person is marked as present for an entire day if they were present in the location at 8:00 pm continuing on to midnight. This means they received safety supervision and possibly received a meal, personal care assistance, and medication administration.
- A person can **NEVER** be marked as present on the day they were admitted to a hospital, a care facility or certain types of camps.
- A person may be marked as present on the day of discharge from a care facility or certain types of camps as long as they arrive home by the time specified above. Verify the correct way to mark a person with the Director of Business.
- Notes for absences in Specialized Residential locations are to be included at the bottom of the Occupancy Log in the space provided.
- If a person supported is on Hospice, care must be coordinated with the Hospice Agency so there is not a duplication of service with the Home Help service. For example, if a Hospice Aid bathes the person three times per week LADD can mark the Personal Care Services Provider Log only on the days bathing was completed by the LADD staff and not the Hospice Aid. This must be noted at the bottom of the Personal Care Services Provider Log, i.e. Sally is now on Hospice; Hospice Aid bathed Sally on the 1st, 4th, 7th etc. etc.
- When a person lives in SIL notes are entered on the Activity Tracking and covers all times a person is not receiving services so there are no special guidelines specific to absences. These notes are referenced for all Contract Agency Billing including Home Help billing.
- CLS and Respite services are entered on Billing Logs as time services were provided so there are no absences to note.
- The Finance Specialist refers to Activity Tracking in order to verify absences for Home Help billing.

Billing Contract Agencies

1. All Occupancy Logs, Billing Logs, Activity Tracking and Billing Worksheets are saved electronically in R:\002. Electronic Occupancy Logs and then divided into folders by region and location. Supporting billing documentation is maintained in the I: Drive.
2. Each Contract Agency utilizes a different online billing system and follows different contract rules for timely filing of claims, appeals and billing corrections. LADD utilizes Business Department personnel to follow all billing standards. It is not possible to include all standards in this section as they are too numerous and are updated frequently.

Billing Contract Agencies for Home Help Services

PREPARATION

1. All Personal Care Service Provider Logs are saved electronically in R:\002. Electronic Occupancy Logs and then divided into folders by region and by program location
2. Managers of each program will ensure the Personal Care Service Log is completed daily throughout the month. If the person received the service according the Time and Task an X is placed in the appropriate date square.

***** IMPORTANT INFORMATION*****

When new time and task information or authorizations are received the Finance Specialist updates the corresponding billing log and informs the Director of Operations and Development so updates to the budget are made.

3. On the 1st day of the month or the first business day following the month of service by 12:00 pm the Manager will have completed review of the Personal Care Service Provider Log for accuracy and completeness and then sign the Log. The Manager will notify their Area Supervisor who will then review the Log to ensure there are no missing signatures or discrepancies The Area Supervisor will then sign and notify the RD the Log is complete.

4. The RD will review all Logs comparing the total minutes billed for that month versus the approved hours/minutes on the Time and Task section at the top of the Log ensuring services have been properly billed. Once RDs have confirmed the total hours/minutes are correct they will email the Finance Specialist.
5. The Finance Specialist will print the completed Personal Care Service Provider Logs and completes billing per county specific guidance.
6. The Finance Specialist will bill other Contract Agencies such as Meridian or Aetna using the approved billing systems, documentation and standards.
7. After billing has been completed the Finance Specialist will enter billing data accordingly in the I:Drive.

PROCESS FOR COMPLETING SPEND DOWNS

1. Spend downs must be faxed to appropriate DHHS office.
2. Proof of Assets/Bank Statement need to be obtained from the Payee and/or LADD for all Berrien and Van Buren Individuals. Cass County individuals do not need bank statements. The Finance Specialist coordinates with the Manager to collect this information.
3. The Finance Specialist will coordinate with the billers to ensure corresponding Contract Agency billing occurs.
4. The Finance Specialist, for each person with a spend down will complete MDHHS Deductible Report. The Finance Specialist will update the Deductible Report (First Page) with the dates of the month that are being billed to the Contract Agency. On the second page on the top right of the Deductible Report, the balance from their bank statements need to be listed. Bank statement totals combined cannot be more than \$2,000.
5. The Finance Specialist will then fax as follows:
 - ❖ Fax to DHS the following documents:
 - ❖ Deductible Report (2 pages)
 - ❖ Bank Statements
 - ❖ DHS FAX cover sheet
 - ❖ Cass County DHHS 269-445-0297/ Berrien and Van Buren counties DHHS 517-346-9888
 - ❖ Cass County Individuals only, need the Spend-Down Billing Sheet faxed to Cass County DHS (Kristy Chaffee). Do not include bank statements or Deductible Reports.
6. The Finance Specialist will maintain a record of all faxed spend downs and other related documentation.

PROCESS OF RUNNING BRIDGE CARDS

Bridge Card Machine and Bridge Card Storage –

- Bridge Cards are stored in a plastic box and locked in a safe in the secure record room at the office.
- Bridge Cards are only accessed when a new card is received or during monthly processing.
- The Bridge Card machine (POS terminal), used to access the benefit is maintained in the Finance Specialist office.

Bridge Cards

1. Upon receiving a new Bridge Card, the Finance Specialist will make a copy of the Bridge Card and the letter it is attached to and file in the Person Supported Administrative Record.
2. Occasionally multiple cards are sent to LADD from DHHS. In these cases, only the Authorized User card in LADD's name will be retained all others cards will be kept separate in the safe. If the only card received is the Bridge Card with the Person Supported name on it then that card will be used.
3. Upon receiving the DHHS notification of the Bridge Card Benefit that amount will be entered into the Person Supported Database.

Running the Bridge Card

- All Bridge Card PIN numbers, DOB or any other numbers associated with access to the benefits on the card are kept in a separate secure database.
 - Any new Bridge Cards are activated and the PIN is changed to the standard PIN used for all cards.
1. Processing Bridge Cards begins on or after the 22nd of each month.

2. Bridge Cards are removed from secure storage, run through the Bridge Card machine and then returned to secure storage. Bridge Cards are not to be left unattended.
3. Amounts transferred off of the Bridge Card are recorded on the Food Stamp Database and the Monthly Living Expense spreadsheet for people who live in Supported Independent Living. Once all Bridge Cards have been processed for a batch total is printed from Bridge Card machine (POS terminal) and reconciled to the total on the Food Stamp Database.
4. All Bridge Cards that have been processed will be verified that batch totals and Food Stamp Data Base totals match. All receipts of transactions are maintained in a separate folder, by month, in the Office.
5. The Food Stamp Database totals are emailed by the Finance Specialist to FOI . All receipts of transactions are also sent to FOI.
6. FOI will make a comparison of the database and receipts to confirm the amounts match and the Bridge Card balance has been taken to zero. Once confirmed FOI will also verify the Food Stamp Database and receipts coincide with the amount deposited into the bank from the Bridge Card machine.

Bridge Card Destruction

- A copy of all letters and Bridge Cards received will be retained in the Person Supported Administrative Record. This is done so there is documentation of the receipt of all cards.
 - Once a person is discharged from services their Bridge Card is deactivated and destroyed. The person and/or their guardian will be notified of the deactivation and destruction of their Bridge Card. They will be informed they will be able to obtain a new card at their local DHHS office. If necessary LADD can assist with transportation to facilitate the expedited receipt of a new Bridge Card.
1. The Bridge Card to be destroyed will be deactivated by calling the number listed on the letter the Bridge Card was attached to when received.
 2. Once the Bridge Card has been deactivated it will be shredded or cut into pieces so that it is no longer recognizable.
 3. The date the Bridge Card has been destroyed is noted on the copy of the letter received from DHHS that the Bridge Card was attached to when originally received. This letter must also be signed by at least two witnesses who have seen the card's destruction.
 4. This dated and signed document is retained in the Person Supported Administrative File indefinitely as documentation the Bridge Card was destroyed.

OPEN ITEMS

An accounting of all open items will be provided by FOI when available. The Business Department will review and make corrections. FOI will be updated on progress towards resolving outstanding issues.

LADD
WE MAKE THE DIFFERENCE



COMMUNICATION

At LADD all employees will use their voice and speak up when they see or hear issues and have ideas on ways to improve services, following the core value; empower by using S.O.U.L. and positive, open communication.

LADD's employee relations policies emphasize open-door practices whereby employees are encouraged to deal directly with their immediate supervisor and other members of management regarding complaints or perceived inequitable conditions of employment in an effort to preserve a positive work environment.

Open, honest communication between managers and employees is a day-to-day business practice. Employees may seek counsel, provide or solicit feedback, or raise concerns within the company.

Management holds the responsibility for creating a work environment where employees' input is welcome, advice is freely given, and issues are surfaced early and are candidly shared without the fear of retaliation when input is shared in good faith.



LADD

WE MAKE THE DIFFERENCE



OPEN DOOR COMMUNICATION POLICY

PURPOSE

The purpose of this policy is to support, promote and preserve the employee and supervisor relationship. Our Core Competencies, which are in every Job Description of every position at LADD demonstrate the importance of open communication and LADD's commitment to this practice.

SCOPE

This policy applies to all employees of LADD.

POLICY

It is the policy of LADD that all employees will use their voice and speak up when they see or hear issues and have ideas on ways to improve services following the core value; empower by using S.O.U.L. and positive, open communication.

STANDARDS AND DEFINITIONS

The company's employee relations policies emphasize open-door practices whereby employees are encouraged to deal directly with their immediate supervisor and other members of management regarding complaints or perceived inequitable conditions of employment in an effort to preserve a positive work environment.

Open, honest communication between managers and employees is a day-to-day business practice. Employees may seek guidance, provide or solicit feedback, or raise concerns within the company.

Management holds the responsibility for creating a work environment where employees' input is welcome, advice is freely given, and issues are surfaced early and are candidly shared without the fear of retaliation when this input is shared in good faith. This is the foundation for continuous quality improvement.

PROCEDURE – Using Your Voice

1. Verbal: At any time, an employee feels a need to discuss concerns; the employee should contact their immediate manager/supervisor. The Human Resource Department is also available to discuss concerns.
2. Written: If the employee would prefer to put their concern in writing, they can email the Human Resource Department or may complete a Confidential Employee Complaint Form and follow the complaint procedure.
3. Employees may use a number of methods to make contact and review questions or concerns; these include;
 - Suggestion Box located in the office and online.
 - Email to Human Resources, CCO or a Director.
 - Call to speak with a Director using the phone numbers posted in locations where staffing supports are provided.
 - Walk in and/or call any LADD corporate office for an appointment to speak with a member of management
 - During question and answer time at training.
 - Through course evaluations.
 - Complaint Form available online.
 - Through Surveys
 - During Family Staff meetings
 - During Staff Council
 - Through Scomm message within Therap.
4. If any employee ever feels retaliated against then it is important to notify the Corporate Compliance Officer. See the Complaint Reporting Policy.



WHISTLEBLOWER POLICY

PURPOSE

The purpose of this policy is to support the organization's goal of legal compliance in all areas of business operations and service delivery. The support of all employees is necessary to achieving compliance with applicable laws and regulations.

SCOPE

This policy applies to all employees of LADD.

POLICY

It is the policy of LADD to adhere to all laws, regulations and contract standards regarding organizational behavior and to encourage any employee who reasonably believes that a policy, practice, or activity LADD engages in is a violation of the law, unethical or inappropriate to report that behavior without fear of retribution.

STANDARDS AND DEFINITIONS:

Whistleblower - A whistleblower is an employee who reports an activity that is illegal, unethical or inappropriate. Examples of such behavior;

- Billing for services not performed or paying for goods not delivered.
- A criminal offence, for example fraud.
- Someone's health and safety are in danger.
- Risk or actual damage to the environment.
- A miscarriage of justice.
- The company is breaking the law
- You believe someone is covering up wrongdoing

Retaliation - Occurs when an employer takes an **adverse action** against a **covered individual** because he or she engaged in a **protected activity**.

- All employees are protected from retaliation. It is the employee's responsibility to bring alleged unlawful activity of LADD to the CCO and provide LADD with a reasonable opportunity to investigate and correct the alleged unlawful activity. Protection is available to employees that comply with this requirement. Any actions or intentions to 'cover up' or failure to report information related to the issue will be appropriately disciplined.
- LADD will not retaliate against an employee for disclosing information that an employee or applicant reasonably believes provides evidence of a violation of any law, rule, regulation, gross mismanagement, gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. One of LADD's core values includes positive open communication at all levels.
- Whistleblowers are protected from retaliation for disclosing information that an employee or applicant reasonably believes provides evidence of a violation of any law, rule, regulation, gross mismanagement, gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. Any employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including separation of employment.
- Directors, officers, employees, and volunteers should share their questions, concerns, suggestions or complaints with someone who can address them properly. The CCO is available at any time.
- **Any employee who intentionally files a false report of wrongdoing will be subject to discipline up to and including separation from employment.**

In order for a person to put forward a claim as a Whistleblower, it must be determined they reported information that led to an act of retaliation by looking at the following:

- A protected activity occurred such as a report to a supervisor was made indicating an illegal, unethical or inappropriate activity occurred.
- An adverse employment action was taken, such as firing or laying off, demoting, denying overtime or promotion, or reducing pay or hours.

A causal connection between the protected activity and adverse action can be made.

Complaint Reporting - It is the responsibility of all employees to immediately report to the CCO, any suspicion of fraud, waste, or abuse in connection with the business of LADD and may do so without fear of retaliation.

Confidentiality – Reports may be submitted on a confidential basis by the employee and will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation. Follow up questions and investigation may not be possible or may be hindered unless the source of the information has been identified.

PROCEDURE

1. The employee should promptly report suspected or actual events to the CCO using published methods such as calling the Compliance Hotline or sending the CCO an email. Refer to the Complaint Reporting Policy for additional information regarding reporting requirements and methods.
2. If the employee is uncomfortable or otherwise reluctant to report to the CCO then the employee can report the event to the Board of Directors or Executive Director.
3. The employee can report the event with his/her identity or anonymously.
4. The employee shall receive no retaliation or retribution for a report. If the employee is found to have been involved in some way with the issue being reported the fact that they reported does not remove them from potential disciplinary action if they are found to be an active participant in the reported issue.
5. The employee will provide details necessary to complete a thorough investigation by the CCO per the Investigation Policy. Investigations must be completed in a timely manner.
6. If the event reported includes a crime against a person or property, such as assault, rape, burglary, etc., it should immediately be reported to local law enforcement personnel.
7. When possible, the employee who reported shall receive a Notice of Findings within five business days of the initial report of the event regarding the investigation, disposition or resolution of the issue.

WE MAKE THE DIFFERENCE



COMPLAINT REPORTING POLICY

PURPOSE

The purpose of the LADD Complaint Reporting Policy is to ensure LADD adheres to all laws, regulations, policies and procedures that apply to or have been adopted by the company. The policy will provide a method of reporting suspected violations, complaints and document appropriate corrective action. Management has the obligation to conduct a prompt, thorough, and impartial investigation into all reports.

SCOPE

This policy applies to all stakeholders including employees, people supported, families, legal guardians, contract agencies and community members.

POLICY

It is the policy of LADD to promote a positive public image that aligns with the mission, vision and values of the company. If any employee or stakeholder reasonably believes that some policy, procedure, best practice, or activity of LADD is not being followed or is in violation of the law, regulation or contract standard a method to report is made available. All reports will be thoroughly investigated, without bias and immediate corrective action will be taken.

STANDARDS AND DEFINITIONS

*****Any complaints that involve fraud, waste, abuse or violations of confidentiality must be reported immediately to the CCO*****

*****Any complaint that involves harassment, retaliation or violence must be reported immediately to the CCO*****

There are several methods to report suspected violations or complaints;

- The LADD Directory – contains the Complaint Form as part of the Compliance and Ethics Program. The LADD Directory is located online.
- Staff Communication Log–contains the Complaint Form in the Postings Section.
- Suggestion Box – located on line and at the company offices.
- Email the Corporate Compliance Officer – email address listed on line and on the Emergency Procedure Responsible Person List at corporatecompliance@laddinc.net
- Call the Corporate Compliance Officer – telephone number available on line and listed on the Emergency Procedure Responsible Person List.
- Call the anonymous hotline and leave a message – telephone number available on line; toll free.
- LADD Privacy Practices – telephone number and address for contacting the Corporate Compliance Officer listed.
- Face to face meeting with a member of Management, Human Resource Director and/or Corporate Compliance Officer– unannounced meetings will be accommodated in most circumstances.
- Call a member of Management – Use the Emergency Procedure Responsible Person List to access the correct number to call.
- New Hire and Annual Training – includes contact information for contacting the Corporate Compliance Officer by toll free number phone, fax or email.
- Complaint Form – the Complaint Form is available on line and in service locations as well as on the people supported website.

A suspected violation, complaint or report is referred to as informal or formal based on the following standard;

- **Informal Complaints** - are generally complaints that are resolved by informal discussions where questions/concerns are raised, policy/procedure is referenced and education and training take place.
- **Formal Complaints** - are made in writing using the LADD Complaint Reporting Form. A person supported may request staff or management to assist them with writing the complaint for them if necessary. This requirement is not meant to limit the ability of a person to make a Formal Complaint but is required so that sufficient detail is available to process the complaint. Formal Complaints should include relevant details, evidence and verifiable facts to support the complaint. It is the inclusion of this level of detail that further serves to differentiate an Informal Complaint from a Formal Complaint. All Formal Complaints will be routed to the CCO.

LADD is structured with 4 different Departments to assist employees and stakeholders; a Corporate Compliance/Business, Quality Assurance/Improvement, Services, and Human Resource Departments. Depending on the issue, more than one department may need to be involved to investigate and resolve the issue. In certain circumstances, it is possible to have a complaint from an employee or stakeholder such as person supported, guardian, family member reviewed by an external reviewer, outside of LADD. The Executive Director or their designee will determine this.

The LADD reporting system is designed with confidentiality and anonymity in mind. Every attempt will be made to assist people with reporting while maintaining confidentiality. This is a critical element of a robust reporting mechanism. However, due to the details of the report and investigative processes the identity of the person reporting may be able to be determined by others involved in the situation and is unavoidable.

In addition, all employees and individual stakeholders such as people supported, guardians and family members are provided with protection so that reports do not result in retaliation or barriers to service.

Routine testing of reporting mechanisms will occur to ensure they are functioning correctly and the Corporate Compliance Officer is receiving reports.

All stakeholders, including employees of LADD must immediately report to the CCO, any suspicion of fraud, waste, or abuse in connection with the business of LADD.

The Corporate Structure and Chain of Communication (following the Chain of Communication below is not a requirement for a compliance issue);

- Program Managers
- Area Supervisors
- Regional Directors
- Director of Operations and Development, Director of Human Resources, Director of Quality Improvement and Director of Business
- Executive Director/Board of Directors – The Corporate Compliance Officer has a direct reporting responsibility to the Executive Director and the Board.
-

PROCEDURE

Reporting failure to follow company policy, procedure or best practice.

1. If an employee or other stakeholder becomes aware of a policy, procedure or practice they feel is not being followed they are expected and encouraged to report the problem or situation to Management via one of the methods specified in the Definitions and Standards section of this policy as an Informal Complaint.
2. In these circumstances it is beneficial for the person reporting, together with Management, to address the Informal Complaint directly since they may be closest to the issue and therefore in the best position to make immediate

corrections. The Mission, Vision and Values is an excellent tool to use in addressing issues since all employees and stakeholders are provided with a copy and expected to align their behavior accordingly. Regardless, all employees are still required to follow reporting requirements as trained i.e. Incident Reports.

3. It is **NOT** the intent of this procedure to limit or restrict reporting but to aid in the timely resolution of complaints. The person reporting may choose to report to any level of Management at any time including the CCO at their discretion using the method that is best for them i.e. telephone, email, text.
4. If it is not possible to address or resolve the Informal Complaint using this approach, then the person will use the chain of communication from the Standards and Definitions section of this policy to guide them to the next available level of Management to address their complaint.
5. If the Informal Complaint has not been resolved or addressed as agreed by the previous two steps a meeting with the person and a Department Director will occur to resolve the issue. The meeting will occur within five business days of the request by the person for a meeting.
6. Documentation of the meeting will be completed by the Department Director and include a summary of the complaint, any additional investigation and review of findings, including steps that will be taken to address the complaint. Documentation will be forwarded to the CCO and the findings will be communicated to the person within two business days of the meeting.
7. If the above steps fail to yield a resolution, the person may contact the CCO for assistance with resolving the complaint. If necessary the CCO, in conjunction with the Executive Director will determine if external review will take place. External review is the final step in an Informal Complaint. The person will then move to the Formal Complaint process. It is not necessary to begin the process as an Informal Complaint. Informal Complaints can be elevated to a Formal Complaint at any time by completing the Complaint Form and submitting it to the CCO.
8. If a person has a Formal Complaint the complaint will be forwarded to the CCO per the Standards and Definitions section of this policy for resolution.
9. The CCO will meet with the person within two business days of receiving the Formal Complaint.
10. Documentation of the meeting will be completed by the CCO and include a summary of the complaint, any additional investigation and review of findings, including steps that will be taken to address the complaint. The Notice of findings will be communicated to the person within two business days of the meeting.
11. If all above steps fail to yield a resolution, the CCO will assist the person to contact the Executive Director who will assist the person to contact the board for review and resolution if necessary.
12. If a conflict of interest is reported that involves the Corporate Compliance Officer, then the Executive Director/Board of Directors can approve an outside reviewer to investigate and report back to the Board of Directors.

Report of suspected violation of law, regulation or contract standard.

1. If a person suspects a violation of law, regulation or contract standard they are expected and encouraged to report the problem or situation to Management via one of the methods specified in the Definitions and Standards section of this policy as well as the appropriate regulatory authority.
2. It is the expectation of Management that all complaints received that are related to violation of law, regulation or contract standard are immediately reported to the CCO who will review with the Executive Director for further action. This may then be reported by a member of Management to the county's designated Recipient Rights Officer, Adult Protective Service, Local Authorities, or Licensing Consultant.

Reporting and grievances by the people supported – Management will assist the person as necessary and/or requested to find available advocacy services for assistance in the complaint process.

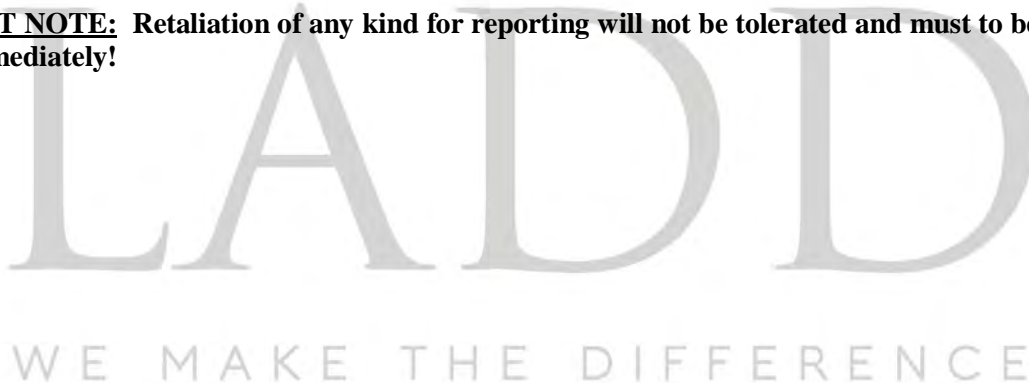
1. If a person supported has an Informal Complaint, they are encouraged to contact the Manager of the support services they receive. When the person supported addresses the complaint with the Manager, they are engaging the person in the best position to provide immediate assistance with their complaint.
2. If it is not possible to address or resolve the Informal Complaint using this approach then the person supported will receive assistance, if necessary, by any LADD employee to use the chain of communication from the

Standards and Definitions section of this policy to guide them to the next available level of Management to address their complaint.

3. If the Informal Complaint has not been resolved or addressed as agreed by the previous two steps a meeting with the person supported and a Department Director will occur to resolve the issue. The meeting will occur within five business days of the request by the person supported for a meeting.
4. Documentation of the meeting will be completed by the Department Director and include a summary of the complaint, any additional investigation and review of findings, including steps that will be taken to address the complaint. Documentation will be forwarded to the CCO and the findings will be communicated to the person supported within two business days of the meeting.
5. If all above steps fail to yield a resolution, the Department Director will assist the person supported to contact the CCO for assistance with resolving the complaint. If necessary the CCO, in conjunction with the Executive Director will determine if external review will take place. External review is the final step in an Informal Complaint. The person supported will then move to the Formal Complaint process. It is not necessary to begin the process as an Informal Complaint. Informal Complaints can be elevated to a Formal Complaint by completing the Complaint Form and submitting it to the CCO.
6. If a person supported has, a Formal Complaint the complaint will be forwarded to the CCO per the Standards and Definitions section of this policy for resolution.
7. The CCO will meet with the person supported within two business days of receiving the Formal Complaint.
8. Documentation of the meeting will be completed by the CCO and include a summary of the complaint, any additional investigation and review of findings, including steps that will be taken to address the complaint. The findings will be communicated to the person supported within two business days of the meeting.
9. If all above steps fail to yield a resolution, the CCO will assist the person supported to contact the Executive Director who will assist the person to contact the board for appeals, review and resolution.

The CCO will keep documentation of all Formal Complaints and complete an analysis as part of the Compliance Report to include the number of complaints received, trends, areas of possible improvement and action taken towards improvement.

IMPORTANT NOTE: Retaliation of any kind for reporting will not be tolerated and must be reported to the CCO immediately!





COMPLAINT FORM

This form provides a process for all stakeholders including employees, people supported, families, legal guardians, contract agencies and community members to file a formal complaint regarding grievances, suspected violations or problems with the organization and its employees, including Management and to receive careful consideration and prompt resolution. All individuals are encouraged to discuss concerns or problems with Management via the informal complaint process whenever possible. The complaint form is available on the LADD website and in all service locations. All formal complaints will be routed to the Corporate Compliance Officer (CCO) utilizing fax, mail, email, or delivered face-to-face. If needed, assistance will be given with completing this form and any LADD employee is able to provide this assistance. The Compliance and Ethics Program provides that all individuals who submit a complaint are protected against retaliation or barriers to services for filing their complaint.

Please fill out this form and submit through any of the above-mentioned methods. You may report with or without using your name. This reporting system is designed with confidentiality in mind. LADD will do its best to restrict your report on a "need to know" basis. No disciplinary action will be taken for merely reporting. For more information please see the CEP. Management has the obligation to conduct a prompt, thorough and impartial investigation.

*Anyone requiring assistance in completing this form may contact a staff member or Management. Staff assisting a person we serve must help the person understand this form and interpret their thoughts, feelings and words as best as possible. *

I. What is the complaint about?

II. Tell us about what happened, when and whom this involves. Please tell us how this made you feel.

III. Please tell us what you would like to see done about this problem and how you think it should be corrected. Attach additional sheets if necessary.

VI. Have you talked with Management?

No Yes If yes, who did you speak with and when was it?

If you have not talked with that person, can you tell us why?

Thank you for bringing your concern to our attention. We will try to resolve your complaint as quickly as possible. Feel free to keep in touch with us during the process. Our experience suggests that first discussing your concern with Management often resolves the complaint.

Signature

Date

*Signature of Person Providing Assistance (if needed)

Date

Send To:

LADD Inc. Corporate Compliance
300 Whitney Street
Dowagiac, MI 49047

Anonymous Reporting: 1-855-607-1737

Fax: 269-782-3828

Email: corporatecompliance@laddinc.net

Management Use

Date Rec'd:

Date Closed:

Tracking #:

Copy to ORR if needed:



DUTY TO WARN POLICY

PURPOSE

To provide direction regarding the notification and/or involvement of the people we support, employees and others when threats of harm are made by people we support or other employees associated with LADD.

SCOPE

This policy applies to all the locations operated by LADD.

POLICY

LADD must act to warn and protect reasonably identifiable victims when a threat of harm is made.

STANDARDS AND DEFINITIONS

None

PROCEDURE

1. When a person receiving services or a member of their immediate family or other credible informant, whether during initial contact or during the course of service, communicates to any employee that a serious threat of physical violence against a reasonably identifiable victim or victims has occurred, then a member of management must be contacted in order to protect the third party.
2. Management will:
 - a. Report the situation to the CCO or the Director of Operations and Development in the CCO's absence.
 - b. Review past and present history.
 - c. Discuss with Supervisors, contract agency, and other applicable agencies to gather information and identify if there is a serious danger to a reasonable identifiable foreseeable victim or victims.
3. If it is decided there is a serious danger to an identifiable/foreseeable victim or victims, then this fact will be documented by the CCO and treated as a HIPAA disclosure per the Notice of Privacy Practices. The CCO will include the rationale, or if it is decided that there is serious danger to a reasonably identifiable/foreseeable victim or victims, the following three actions must be taken:
 - a. Make reasonable efforts to notify the intended victim or victims. Contact may be made through telephone, visitation or other methods of communication.
 - b. Documentation in the Individual records is required. It must include specific efforts to contact the potential victim, times and dates of these attempts written in the progress notes, retaining a copy of written correspondence, and contact with family or friends with specific times and names noted in the progress notes.
 - c. Contact the local law enforcement agency having jurisdiction where the possible victim resides. Record in the clinical record the name of the person to whom the report was made with the date, time, and content released. Involuntary hospitalization of the client does not discharge the duty to warn and protect which includes notifying law enforcement.
4. In a situation that involves "substantial probability of harm" as determined by the CCO and/or contract agency, confidentiality of individuals involved will be waived and the appropriate agencies or individuals will be notified immediately.
5. Only the minimum amount of information necessary to protect the intended victim or victims shall be released.
6. This exception to confidentiality must be carried out with care and consideration, with the maintenance of the public safety and therapeutic relationship as objectives.
7. If the situation involves a reasonable cause to suspect child or vulnerable adult abuse, the CCO will make a report to the Department of Health and Human Services (DHHS) LADD Inc management employees will also immediately make a verbal report to DHHS per the policy on Incident Reporting Investigation Policy on Unusual and Critical Incidents at Central Reporting at 855-444-3911. A written report via DHHS form 3200 may be required at this time.



CLOSING

LADD is committed to all elements of the CEP and continuously reviews and revises policies, procedures and practices to remain compliant with all laws, regulations and standards of best practice. LADD is committed to standards for ethical practices concerning staff, Management and all operations of LADD. Inclusive in these is the expectation that support services are provided responsibly, fairly and with awareness of the surrounding community and provide services consistent with LADD Mission, Vision and Values.

If at any time one of the many LADD stakeholders has a question or concern they can use the information below to make contact.

LADD Corporate Compliance
300 Whitney Street
Dowagiac, MI 49047

Office number: 269-782-0654
Fax: 269-782-3828

Anonymous Reporting: 1-855-607-1737
Email: corporatecompliance@laddinc.net



LADD

WE MAKE THE DIFFERENCE