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;

- Unknowing- 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 be 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.