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.

WE MAKE THE DIFFERENCE

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 thee 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