AHRC NYC Compliance Training for Contractors

Rev. 03.17.2023

False Claims Act

- The False Claims Act is a federal law which prohibits knowingly or negligently submitting false claims.
- AHRC NYC upholds all aspects of the False Claims Act including but not limited to the Whistle Blower Provisions, anti-retaliation, and anti-intimidation standards.
- Failure to comply with the False Claims Act bears significant financial penalties in addition to repayment three times the amount of the original false claim.
- Some examples of False Claims are to:
  - bill for services that were not provided.
  - provide & bill for unnecessary services.
  - bill for a time period longer than the service was provided.
  - complete documentation with little or no factual basis.
  - fail to document the actual time spent on a service.
  - keep poor records.
  - Unbundling and up coding.

Whistleblower Protection Act

- Whistleblowers are protected from retaliation for disclosing information that they 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.

- If someone “whistles” in good faith, AHRC NYC cannot retaliate or intimidate them. The person may also be entitled to a percentage of the funds recovered.

Whistleblower Definitions

- "*Good Faith*" participation or reporting includes, but is not limited to:
  - reporting actual or potential issues or concerns
  - cooperating or participating in the investigation of such matters
  - assisting with or participating in self-evaluations, audits and/or remedial actions; and reporting to appropriate officials as provided in New York State Labor Law

- *Intimidation* is defined as including but not limited to any act to manipulate a person or intentionally cause feelings of fear or inadequacy subsequently deterring that person from reporting breach of the law.

- *Retaliation* is defined as any adverse action against the individual because of the individual's good faith report of a compliance concern or participation in a compliance investigation.

HIPAA/FERPA & eHIPAA/eFERPA

- Health Insurance Portability and Accountability Act (HIPAA) is a federal law imposed on all providers of healthcare & their business associates which protects the privacy & security of protected health information (PHI).
- The Family and Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy/security of student education records.
- Under HIPAA, PHI/E-PHI may not be given to anyone without the individual's/representative's written authorization , except as it is necessary for the agency's normal treatment of the individual receiving services, processes leading to the payment for services to the individual, operations, such as quality assurance, compliance, etc.
- Disclosure of PHI requires notification to the agency's Privacy Officer utilizing the agency forms and expressed approval from Privacy Officer.
- HIPAA Security Rule (E-HIPAA) defines the standards which require covered entities to implement basic safeguards to protect electronic Protected Health Information (e-PHI)
- E-PHI is computer based health information that is used, created, stored, received or transmitted by AHRCNYC using any kind of electronic information resource
- PHI is not to be discussed in public (ex. Hallways or elevators), never should be left unattended (ex. In the fax machine or copier or a file left unattended), computers left unprotected (failing to log out or using a password).
- Reporting of a Potential Breach: Any workforce member who knows, believes, or suspects that a privacy or security breach of PHI has occurred must immediately follow their department's protocol for reporting the suspected breach to the Privacy Officer or Security Officer depending on the type of breach.

Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act")

While HIPAA protects the PHI of those receiving services from AHRC NYC, the SHIELD Act (which became effective 03/21/2020) broadens the definition of what is considered PHI (as defined below) and its protections are extended, but not limited to, AHRCNYC employees, contractors, interns, and business associates.

- **Broadening the Definition of "Private Information."**
  - include biometric information and username/email address in combination with a password or security questions and answers. It also includes an account number or credit/debit card number, even without a security code, access code, or password if the account could be accessed without such information.
- **Expanding the Definition of "Breach."**
  - unauthorized "access" of computerized data that compromises the security, confidentiality, or integrity of private information, and it provides sample indicators of access. Previously, a breach was defined only as unauthorized acquisition of computerized data.
- **Expanding the Territorial Scope.**
  - now any person or business that owns or licenses private information of a New York resident. Previously, the law was limited to those that conduct business in New York.
- **Imposing Data Security Requirements.**
  - requires companies to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information. A company should implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal.

Basic Compliance

- Always print, sign, and date all of your documents.
- Never back date any documents.
- All documents are to be completed contemporaneously.
- Always use blue ink pen to write.
- When making corrections, draw a single line across the mistake and write correction in the space above or below the crossed-out mistake and initial.
- Writing must always be legible.
- Never print or sign someone else's name.

Corporate Compliance

- The Chief Compliance Officer and Privacy Officer is Sandra Moody (email: Sandra.Moody@ahrcnyc.org)

- For security related matters, our Security Officer is John DeFreitas (email: John.DeFreitas@ahrcnyc.org)

  Please complete an IT ticket for any known security breaches.

- For Privacy related matters, please email: privacyofficer@ahrcnyc.org

- To report a compliance situation, you may either use the compliance hotline number: (212)780-4485 or submit an anonymous form using the following link: https://www.ahrcnyc.org/compliance-practices/submit-a-compliance-violation-report/