LAUNCH
Fueling Individualized Learning

Date: 9/23

Policy Name: Corporate Compliance Plan

Policy Number: 506

CORPORATE COMPLIANCE PLAN

LAUNCH has developed a Corporate Compliance plan in an effort to comply with applicable State and Federal laws. The purpose of an effective corporate compliance plan is to reduce waste and prevent fraud and abuse. Adhering to LAUNCH's corporate compliance program is the responsibility of all affected individuals including; employees, the chief executive and other senior administrators, managers, contractors, agents, subcontractors, independent contractors, and governing body and corporate officers. LAUNCH is committed to providing quality services and billing for services in a legal and ethical manner to ensure that the agency's reputation is protected, and the agency's mission is attained.

Mission Statement:

LAUNCH offers person-centered services that empower individuals of all ages and abilities to reach their full potential as part of our shared community. Services are provided with dedication, compassion, innovation, and commitment.

Board of Directors Endorsement

The Board of Directors is committed to ensuring LAUNCH's compliance with all applicable rules and laws, which govern compliance. The Board of Directors has approved LAUNCH's Corporate Compliance plan and have an active role in the oversight of the implementation of the Corporate Compliance plan. The Board's Audit and Finance Committee meets with the Compliance Committee of the Agency quarterly to review and support Compliance needs.

The Board of Directors' orientation process includes training about the corporate compliance program and the governing body's responsibility to ensure that the agency maintains proper procedures and documentation. Board Members receive Compliance Training annually.

Table of Contents

b. Federal False Claims Act
c. New York State False Claims Act
d. Whistleblower
e. New York Labor Act Section 740
f. New York Labor Act Section 741
g. NYS Medicaid Inspector General Act of 2006
h. Health Insurance Portability and Accountability Act of 2006

4. Exclusion Screening and Background Checks
5. Self-Disclosure
6. Billing and Financial Reporting Records
7. Conflict of Interest
8. Compliance Agency Policies
    a. Compliance Investigation
    b. Compliance Training and Education Plan
    c. Conflict of Interest
    d. Disciplinary, BOD
    e. Disciplinary Policies, Human Resources
    f. Disciplinary, Vendors and Contractors
    g. Exclusion Screening
    h. False Claims
    i. Idenitification of Compliance Risk Areas
    j. Internal Audits
    k. Medicaid Pre-billing Audit
    l. Non-Retaliation and Non-Intimidation
    m. Policy on Policies
    n. Records
    o. Self-Disclosures
    p. Standard of Conduct
    q. Subpoena and Search Warrant
    r. Unannounced Visit by Auditor or Investigator
    s. Whistleblower

Definitions:
"Affected persons": All persons who are affected by LAUNCH's risk areas including the employees, the chief executive and other senior administrators, managers, contractors, agents, subcontractors, independent contractors, and governing body and corporate officers.

"Compliance Officer": Oversee the Agency's quality assurance, corporate compliance, service review, participant satisfaction and staff training activities with the support of Agency's Executive Director and Associate Executive Director. Serve as LAUNCH's Corporate Compliance Officer and Privacy Officer. Oversee the performance outcomes of the agency as it related to valued based outcomes and managed care. LAUNCH's Board of Directors has designated the Associate Executive Director of Quality and Performance from AccessCNY as the agency's Compliance Officer with the assistance of LAUNCH's Executive Director and Associate Executive Director. *See job description forAccessCNY's Associate Executive Director of Quality and Performance at AccessCNY.*

"Compliance Committee": LAUNCH is committed to ethical and legal conduct while providing quality services. This Committee is responsible to collaborate and support the agency's Corporate Compliance Officer to ensure the written policies and procedures, the required standards of conduct are current, accurate, and complete, and that the required compliance training topics are completed timely. This Committee serves in an advisory capacity as Committee to LAUNCH ("Agency") to coordinate with the Compliance Officer to ensure the Agency is conducting business in an ethical and responsible manner consistent with the Compliance Plan. *Refer to Compliance Committee Charter.*

COMPLIANCE PLAN ELEMENTS

LAUNCH is committed to ensuring compliance with all applicable laws and regulations. LAUNCH's Corporate Compliance Plan complies with the Office of the State Medicaid Inspector General's eight required elements and shall be applicable to:

- Billings
- Payments
- Medical necessity and quality of care
- Governance
- Mandatory reporting
- Credentialing
- Ordered Services
- Contractor, subcontractor, agent, or independent contract oversight; and
- Other risk areas that are or should with due diligence be identified by LAUNCH

1. Designation of a Compliance Officer and Compliance Committee:

LAUNCH's Board of Directors has designated the Associate Executive Director of Quality and Performance from AccessCNY as the agency's Compliance Officer. The Compliance Officer reports directly to the Executive Director and has unrestricted access to the Board of Directors related to Compliance.

The Committee and Officer are responsible for reviewing compliance investigations, monitoring audit and risk trends, and ensuring that the agency's compliance plan meets all required elements. The Compliance Committee Charter identifies member responsibilities and is reviewed annually. The committee reports directly and is accountable to the Executive Director and the Audit and Finance Committee of the Board of Directors.

Responsibilities of the Compliance Officer are outlined in the AccessCNY's Associate Executive Director of Quality and Performance job description.

The Compliance Committee will coordinate with the Compliance Officer and assume the duties outlined in the Compliance Committee Charter(Policy #506A).

2. Written Policies and Procedures:

LAUNCH has developed several policies and procedures as part of the agency's compliance plan in compliance with and under the guidance of the Office of Medicaid Inspector General (OMIG). LAUNCH has also developed a Compliance Code of Conduct that all employees and Affected

Individuals are required to adhere to. LAUNCH's compliance policies and procedures include, but are not limited to compliance program education, internal and external audits, billing, State and Federal False Claims Act, reporting and investigating compliance issues, return of overpayments, non-intimidation and non-retaliation, record retention and destruction and protection and security of information in compliance with HIPAA and FERPA laws.

When contracting with Medicaid Managed Care Organizations, LAUNCH will adhere to all requirements set forth in each contract.

All compliance policies will be reviewed at least annually to determine:

a) if all policies, procedures and standards of conduct have been implemented;
b) whether affected individuals are following the policies, procedures and standards of conduct;
c) whether policies, procedures and standards of conduct are effective; and
d) whether any updates are required.

Compliance Policies are available online at www.LAUNCHCNY.org. Employees have access to policies through the Agency Public Drive. Compliance Policies are included herein and part of this policy herein. HR policies are also available on the LAUNCH ADP home page.

3. Training and Education:

All LAUNCH employees, interns, students and volunteers working in a Medicaid billable program receive training on the agency's Compliance Plan, Federal and State False Claims Act, Whistleblower Protections and HIPAA Privacy and Security requirements during orientation and annually. Board members receive training on LAUNCH's compliance plan during Board orientation and then during the annual presentation by the Compliance Officer. All other Affected Individuals receive training upon commencement of a new contract. All employees and affected individuals are required to sign an attestation that they received and understand the training and will not participate in or cover up fraudulent activities. After the initial orientation training, LAUNCH's Corporate Compliance and HIPAA training is provided to all employees and affected individuals on an annual basis.

Compliance training remains a priority as a standing item for individual program staff meetings as well as bi-monthly Management team meetings. Monthly Compliance emails are sent to managers identifying topics to focus on that month at staff meetings. Those topics are reinforced and discussed at Management team meetings. As new regulations are released, this information is shared with the applicable programs and discussed during regular compliance meetings.

Refer to the agency's compliance and education plan for additional information(Policy #511)

4. Communication Lines to the Compliance Officer:

Reporting of compliance issues and/or suspected fraud is the responsibility of all LAUNCH employees and Affected Individuals. The Compliance Officer has been designated as the contact for complaints, questions, suggestions and reporting of compliance issues. All LAUNCH employees and affected individuals are required to report any misconduct, fraudulent acts and/or compliance issues that they witness, suspect or are asked to participate in or cover up. Reports can be made to a supervisor or directly to the Compliance Officer. Reports can be made in person, by phone or email or via the LAUNCH Compliance Hotline. The Compliance Hotline is

a voicemail box and can be accessed directly at **(315) 410-3333**. All reports made to the hotline can be made anonymously as there is no way to identify the caller or the number the call is being made from. Hotline information is available on LAUNCH's website.

Upon receipt of a question or concern, any supervisor or director shall document the issue at hand and promptly report to the Compliance Officer.

Any questions or concerns relating to potential non-compliance by the Compliance Officer should be reported immediately to the Executive Director.

All Medicaid recipients have access to the Compliance Officer's contact information on the website and through intake and annual paperwork.

5. Disciplinary Policies:
Corporate Compliance is an expectation of all LAUNCH employees, Board Members, and Affected Individuals. The agency has developed disciplinary policies that provide the potential consequences of non-compliance for employees, the Board of Directors, and other Affected Individuals such as contractors and vendors.

LAUNCH is committed to ensuring that the discipline for non-compliance is enforced in a fair, consistent, and firm manner at all levels of the organization. Employees and Affected Individuals who fail to comply with LAUNCH's Compliance Code of Conduct, Compliance Plan and standards, or who have engaged in conduct that has the potential of impairing LAUNCH's status as a reliable, honest, and trustworthy service provider will be subject to disciplinary action, up to and including termination of employment, contract, assignment or association with LAUNCH. All Affected Individuals are expected to assist as needed in any compliance investigations.

Disciplinary actions will also be taken for anyone who participates in non-compliant behavior or activities, encourages, directs or facilitates non-compliant behavior, participates in the cover up of such activities or fails to report such activities after witnessing or becoming aware of them. Anyone substantiated for fraud will be terminated.

Managers and supervisors will be disciplined for failure to adequately instruct their subordinates, or for failing to detect noncompliance with applicable policies and legal requirements, where reasonable diligence on the part of the manager or supervisor would have led to the earlier discovery of any problems or violations and would have provided LAUNCH with the opportunity to correct them.

Human Resources policies and Disciplinary Policies for Employees(Policy #1009) located herein on the ADP Home page>Forms Library and the Agency Public Drive.
Disciplinary Policy for the Board of Directors(Policy #1010) is located herein in the Agency Public Drive and is provided to each board member.
Disciplinary Policies for Affected Individual herein on Agency Public Drive.
LAUNCH's Code of Conduct(Policy # 518) policy is located herein at ADP home page>Forms Library and Agency Public Drive.

6. Auditing and Monitoring

An ongoing auditing and monitoring system, implemented by the Compliance Officer and in consultation with the Compliance Committee, is an integral component of the agency's auditing and monitoring systems. This ongoing evaluation shall include the following:

- Review of relationships with third-party contractors, specifically those with substantive exposure to government enforcement actions;
- Compliance audits of Corporate Compliance policies and standards; and
- Review of documentation and billing relating to claims made to federal, state, and private payers for reimbursement, performed internally or by an external consultant as determined by Compliance Officer and Compliance Committee.

LAUNCH has developed a system for self-monitoring to ensure that services are provided, and claims are billed in compliance with applicable rules and regulations as well as in compliance with the agency's Best Practices.

The agency has developed a risk assessment that each department completes annually. The Compliance Officer and Compliance Committee review the assessments and then prioritize risk of all agency programs. The Compliance Officer completes a work plan based on the results of the risk assessments that is shared with all agency programs for implementation. The Quality Enhancement department at AccessCNY has developed audit tools for each program to ensure compliance with applicable rules and regulations. Billing audits are conducted monthly to ensure all billing requirements are met. *See policy 514.*

Deficiencies from external audits are also monitored by the Quality Enhancement team to ensure deficiencies are corrected.

Compliance meetings are held regularly with program staff to review trends identified in internal and external audits, investigation findings, updated regulations, status of the compliance work plan, status of high-risk programs, and other related compliance activities. Programs are also encouraged to complete peer audits and those results are shared with the AccessCNY Consulting QE Department.

Sometimes internal audits and/or complaints reveal documentation and/or billing errors that require further investigation, return of overpayments and/or self-disclosure to the Office of Medicaid Inspector General.

LAUNCH complies with any requests from Medicaid Managed Care Organizations according to the requirements outlined in the contract.

All compliance concerns are shared with the compliance committee quarterly.

Exclusion screenings(*Policy #512*) are conducted according to the Exclusion Screening policy. Any concerns are reported to the Compliance Officer for further investigation and follow-up.

Please refer to the following Audit Policies(Policy #1501) herein in the Agency Public Drive.

7. Responding to Compliance Issues:
LAUNCH takes all reports of non-compliance seriously and has established a procedure for investigating compliance issues. Please refer to the Compliance Investigation policy *(Policy #510)*

When an individual makes a complaint or a compliance issue is discovered, the Compliance Officer initiates an investigation immediately; the type of investigation is dependent on the nature of the complaint.

The Compliance Officer, in conjunction with legal counsel as appropriate, shall ensure that all reports of suspected or actual non-compliance with LAUNCH's Compliance Code of Conduct, Compliance Plan, and compliance policies are thoroughly investigated and corrective actions are taken as appropriate.

Information obtained during a compliance investigation is confidential and only shared with the appropriate Management personnel, as necessary. LAUNCH may be required to disclose information obtained in an investigation when outside agencies such as OMIG, law enforcement, OPWDD, or OMH become involved.

The Compliance Officer shall maintain a record of the investigation, including copies of all pertinent documentation for ten years. The investigation may include, but is not limited to, the following:

- Interviews with individuals having knowledge of the facts alleged;
- A review of documents;
- Root cause analysis; and
- Legal research and contact with governmental agencies for the purpose of clarification.

The investigation record is confidential and will not be released without the approval of the Executive Director or legal counsel.

The Compliance Officer will ensure that corrective action plans are developed and implemented for all confirmed issues of non-compliance.

The Compliance Officer shall report quarterly to the Compliance Committee regarding each investigation conducted.

The Compliance Officer shall report compliance activity to the Board of Directors in a quarterly written report, including reports of non-compliance and investigative findings.

If LAUNCH identifies that an overpayment was received from any third-party payer, the appropriate regulatory (funder) and/or prosecutorial (attorney general/police) authority will be appropriately notified with the advice and assistance of counsel when necessary. It is Agency policy to not retain any funds that are received as a result of overpayments. In instances where it appears that an affirmative fraud may have occurred, appropriate amounts shall be returned after consultation and approval by involved regulatory and/or prosecutorial authorities. Systems shall also be put in place to prevent such overpayments in the future.

Statutory Guidelines

LAUNCH is committed to compliance with all State and Federal laws and regulations. Compliance with the following federal and state laws and regulations will be adhered to at all times. Affected individuals are encouraged to reach out to the Compliance Officer with any concerns.

Deficit Reduction Act of 2005

Chapter 3 of the Deficit Reduction Act (DRA) includes several provisions intended to improve 'payment integrity' in the Medicaid program. Section 6032 requires health care organizations to specifically inform employees about the federal False Claims Act, and similar state laws, and about the whistleblower protections incorporated into these laws.

Federal False Claims Act

The False Claims Act, 31 U.S.C. 3729 *et seq.,* is a federal law that imposes liability on any person or entity who submits a claim to the federal government that they know (or should have known) is false. This act is designed to prevent and detect fraud, waste and abuse in federal healthcare programs, including Medicaid and Medicare.

New York State False Claims Act (State Finance Law §§187-194)

The State False Claims Act imposes fines and penalties on individuals and agencies that file false and fraudulent claims for payment from any state or local government, including health care programs such as Medicaid.

LAUNCH's False Claims Act Policy(Policy # 513) is aligned with the NYS False Claims Act and the Federal False Claims Act and is contained herein on the Agency Public Drive.

Whistleblower or "Qui Tam" Provisions

In order to encourage individuals to come forward and report misconduct involving false claims, the False Claims Act contains a "Qui Tam" or whistleblower provision. The False Claims Act prohibits discrimination by the agency against any employee for taking lawful actions under the False Claims Act.

LAUNCH's Whistleblower policy(Policy #517) is contained herein on the Agency Public Drive.

New York Labor Law §740

An employer may not take any retaliatory personnel action against an employee, former employee or independent contractor if the person discloses information about the employer's policies, practices, or activities to a regulatory, law enforcement, or other similar agency or public official. This includes actions that would discriminate against an employee or former employee or adversely impact a former employee's current or future employment.

New York Labor Law §741

Under this law, a healthcare employer may not take any retaliatory action against an employee if the employee discloses certain information about the employer's policies, practices, or activities to a regulatory, law enforcement, or other similar agency or public official. Protected disclosures are those that assert that, in good faith, the employee believes constitute improper quality of patient care.

LAUNCH's Non-Intimidation and Non-Retaliation Policy(Policy #520) is attached hereto on the Agency Public Drive.

NYS Medicaid Inspector General Act of 2006

This legislation (Chapter 442 §363-d) requires that medical assistance providers must have a corporate compliance program minimally applicable to billings to and payments from Medicaid. This Compliance Plan complies with NYS Medicaid Inspector General Act of 2006. Employees are to be encouraged to participate in the corporate compliance program with policies of both non-retaliation and non-intimidation for coming forward and disciplinary action for failing to do so.

Privacy & Confidentiality

Health Insurance Portability and Accountability Act of 1996

This legislation was intended to enhance the privacy and security of medical information while streamlining the health insurance industry. It applies to all medical providers, insurance companies, and all other entities with access to 'protected health information.' Medicaid has released the code sets to be used in New York State.

LAUNCH is committed to complying with all laws protecting the confidentiality of all individuals' health information, including the Health Insurance Portability and Accountability Act (HIPAA) and HITECH Omnibus Rule, the Family Educational Rights and Privacy Act (FERPA), and the Stop Hacks and Improve Electronic Data Security Act (SHIELD). All employees, interns, volunteers, students, contractors, Business Associates and Board members are expected to adhere to the agency's HIPAA and FERPA standards and procedures. The Associate Executive Director of Quality and Performance has been designated as the agency's Privacy Officer. The Privacy Officer is responsible for monitoring disclosures of individual's PHI (Protected Health Information) and ensuring that the agency's HIPAA and FERPA procedures are followed. All individuals receiving services are given a copy of the agency's Privacy Practices notice during the intake process. The agency's Privacy Practices notice is also available on LAUNCH's website and individuals may request a written copy from a supervisor or the Privacy Officer at any time.

Agency Confidentiality Policy (Policy #507) is located herein on the Agency Public Drive.

Exclusion Screening and Background Checks

LAUNCH will ensure compliance with all federal and state laws and regulations regarding exclusion screening. LAUNCH will not employ, contract with or conduct business with an individual or entity excluded from participation in state or federally sponsored health care programs such as Medicare and Medicaid. LAUNCH will conduct exclusion screening checks on all employees, consultants, vendors, and Board members initially and monthly to ensure compliance with all federal and state laws and regulations regarding exclusion screening.

The Exclusion Screening policy(Policy #512) is contained herein on Agency Public Drive.

Self-Disclosure

LAUNCH is committed to ensuring that the agency's documentation, coding and billing practices comply with all federal and state laws and regulations. LAUNCH prohibits the intentional submission for reimbursement of any claim that is false, fraudulent or fictitious.

At times, LAUNCH may receive overpayment for services. **When the overpayment is considered to be a minor error, LAUNCH will return the overpayment through the process of adjusting or voiding the claim. When it is determined that the overpayment is more significant or systemic, LAUNCH will self-disclose the overpayment to the Office of the Medicaid Inspector General. Issues appropriate for disclosure may include, but are not limited to:

- Substantial routine errors
- Systemic errors
- Patterns of errors
- Potential violation of fraud and abuse laws

In accordance with the Affordable Care Act Section 6402 and New York Social Service Law §363-d, overpayments will be reported and returned by the later of:

- 60 days after the date on which the overpayment was identified; or
- The date any corresponding cost report is due, if applicable.

The Self Disclosure policy(Policy #515) is contained herein on Agency Public Drive.

Billing and Financial Reporting and Records

LAUNCH is committed to ensuring that the agency's documentation, coding and billing practices comply with all federal and state laws, regulations and guidelines. Furthermore, LAUNCH is committed to ensuring against the accidental submission of any claim that is false or inaccurate. All LAUNCH employees and contractors must prepare and submit documentation and billing that is honest and accurate. Billing will only be submitted for actual services provided, which also includes documentation containing all required elements to support the billing. LAUNCH has developed systems to ensure that LAUNCH only bills and receives payment for services provided and supported by the required documentation. Any employee or contractor who knowingly presents or causes to be presented, claims for payment or approval which are false, fraudulent, or fictitious, will be subject to disciplinary action up to termination and/or prosecution.

LAUNCH is committed to creating and maintaining complete and accurate financial records and reports. LAUNCH's financial statements and reports are prepared in accordance with applicable laws, with accepted accounting principles, and are subject to external audits by an independent auditing firm.

***LAUNCH will follow any updated guidance that OMIG releases regarding disclosures.*

Conflict of Interest

LAUNCH is committed to ensuring compliance with all required federal and state laws regarding making transparent and ethical business decisions. All employees and members of the Board will disclose real and potential conflicts of interest and refrain from participation in any decisions on matters that involve a real conflict of interest or the appearance of a conflict pursuant to the Agency Conflict of Interest Policy.

The Agency Conflict of Interest Policy(Policy #1001) is located herein on Agency Public Drive.

Compliance Plan Tracking

Date: Review	Modifications (y/n)	Section(s) Modified	Date: BOD Approval	Date: Effective	Date: Affected Individual Notification	Signature: Compliance Officer
6/22/23	Y	Overhaul of plan				

LAUNCH
Fueling Individualized Learning

Policy Name: Corporate Compliance Plan-committee charter ***Date: 9/23***

Policy Number: 506A

Corporate Compliance Committee Charter

Purpose: Launch is committed to ethical and legal conduct while providing quality services. This Committee is responsible to collaborate and support the agency's Corporate Compliance Officer to ensure the written policies and procedures, the required standards of conduct are current, accurate, and complete, and that the required compliance training topics are completed timely.

This Committee serves in an advisory capacity to the Board of Directors as a Committee to LAUNCH ("Agency") to coordinate with the Compliance Officer to ensure the Agency is conducting business in an ethical and responsible manner consistent with the Compliance Plan.

Responsibilities: Support the quality of services provided through the following responsibilities:

1. Policies:
   - 1.1. Committee will review all Corporate Compliance policies annually.
   - 1.2. Provide drafting support, when requested, for new or revising policies related to compliance.
   - 1.3. Coordinate with compliance officer to ensure written policies and procedures, and standards of conduct are current, accurate and complete, and that required trainings are timely completed.

2. Corporate Compliance Plan:
   - 2.1. Ensure the goal of the Corporate Compliance Plan is designed and implemented to prevent, detect, and correct non-compliance with Medicaid program requirements, including fraud, waste, and abuse.
   - 2.2. Review and ensure that the Agency has effective systems and processes in place to identify compliance program risks, overpayments, and other issues, and effective policies and procedures for correcting and reporting such issues.
   - 2.3. Annually review Corporate Compliance Plan for completion, efficiency, and regulation compliance.
   - 2.4. Annual review of compliance work plan.

3. Communication:
   - 3.1. Coordinate with compliance officer to ensure communication and cooperation by affected individual on compliance related issues, internal or external audits, or any other function or activity required.

3.2. Advocate for sufficient funding and resources that allow compliance officer to fully perform responsibilities.
3.3. Collaborate with compliance officer and report compliance issues that arise to the Executive Director and Board of Directors quarterly.

4. Miscellaneous:
   4.1. Ensure all levels of the organization, including the Board of Directors, support the compliance program.
   4.2. Promote adherence to LAUNCH's legal and ethical obligations.
   4.3. Identify and discuss remedial actions to avoid the repeat of incidents.
   4.4. Discuss disciplinary standards and policies related to Compliance.
   4.5. Review this Charter at a minimum, annually.

Accountability: The Compliance Committee shall report directly and be accountable to the Chief Executive Officer and the Agency Board of Directors through the Audit and Finance Committee of the Board. The Compliance Committee of the Agency designee reports to the Audit and Finance Committee of the Board; the Chair of the Audit and Finance Committee of the Board reports (with support of the Compliance Committee designee) to the agency Board.

Composition: Members will represent the range of LAUNCH staff; the Board of Directors shall designate no less than 3 individuals appointed by the Board to serve on the committee. Corporate Compliance officer will be a committee member. Executive Director and Associate Executive Director will attend quarterly compliance committee meetings. Staff Members must be, at a minimum, a senior manager, and will serve at a variety of Agency work-areas.

Slate: No fewer than three and no more than twelve members.

Term of Service: Annually a Committee Chair will be designated; no term limits for role. The Committee Chair can be the Corporate Compliance Officer. Annually a Secretary will be designated for note taking; no term limits for role.

Non-Intimidation and Non-Retaliation Policy: Compliance is an expectation of all LAUNCH employees, volunteers, intern, students and Board members and LAUNCH encourages everyone to report issues of non-compliance and fraudulent activities without fear of retaliation or intimidation. LAUNCH has developed a Whistleblower Protection policy to prevent intimidation or retaliation for reports made in good faith. If an employee believes that they have experienced retaliation or negative consequences for making a report, filing a complaint or participating in an

investigation; they should contact the Human Resource Director and/or Compliance Officer for further investigation and action.

Meeting Schedule: The committee shall meet quarterly in collaboration with the Audit and Finance Committee of the Board, or more frequently and independently, if needed.

Reviewed and Approved date:

LAUNCH
Fueling Individualized Learning

Policy Name: HIPAA/HI-TECH-Health Insurance Portability and Accountability Act

Date: 12/1/22

Policy Number: 507

Policy

This policy applies to **all** agency staff members to include employees, trainees, volunteers, consultants, contractors and subcontractors at the agency.

The Privacy Rule protects all "individually identifiable health information" held or transmitted by LAUNCH or its business associates, in any form or media, whether electronic, paper, or oral.

"Individually identifiable health information" (further defined below) is information, including demographic data, that relates to:

- The individual's past, present or future physical or mental health condition
- The provision of service to the individual, or
- The past, present, or future payment for the provision of service to the individual

.

In LAUNCH, Protected Health Information (PHI) is information pertaining to the care, treatment and service provision to an individual that identifies or tends to identify such individual.

All agency staff is generally expected to limit their uses and disclosures of protected health information, and requests for protected health information, to the minimum amount of information necessary to perform their duties for the agency. **This general expectation does not mean that agency staff should restrict exchanges of information required in order to serve clients quickly and effectively.**

Definitions

PRIVACY RULE applies to ALL forms of PHI: electronic, written, oral.
The Privacy Rule sets the standards for use and disclosure of PHI/clinical information and to assure individual rights.

SECURITY RULE ONLY applies to electronic, including PHI that is created, received, maintained, or transmitted. This rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards for protecting e-PHI. The Security Rule is "flexible and scalable to allow covered entities

to analyze their own needs and implement solutions appropriate for their specific environments".

HITECH ACT (Health Information Technology for Economic and Clinical Health Act) is part of the American Recovery & Reinvestment Act of 2009 (ARRA) and contains incentives to accelerate use of electronic health record systems among providers.

HITECH also:

- Amends HIPAA to include breach reporting and notification requirements
- Significantly increases civil and criminal penalties for violations, extends them to individuals and business associates
- Enhances state & federal enforcement capabilities
- Expands the scope of HIPAA provisions directly applicable to Business Associate

FINAL OMNIBUS RULE of 2013: This Rule added a change in requirements for Business Associates of covered entities, and puts responsibility for ensuring HIPAA-HITECH compliance with the Business Associate. This Rule also emphasized enforcement activity and penalties associated with violations of HIPAA-HITECH requirements.

PHI (Protected Health Information): As defined in the federal HIPAA Privacy and Security Rules at 45 CFR 160.103, includes individually identifiable health information that is transmitted or maintained electronically or in any other form or media, including paper.

- "is created or received by a health care provider, health plan, public authority, employer, life insurer, school or university, or health care clearinghouse: and
- "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual."
- "that identifies the individual" or can be used to identify an individual.

In LAUNCH, PHI is also known as "clinical information" pertaining to the care, treatment and service for an individual that identifies or tends to identify such individual.

PHI: IDENTIFIERS: List of 18 Identifiers (NOTE: The presence of one or more of these PHI identifiers does not necessarily constitute a breach; Breach determination process described later in this document):

1. Names
2. All geographical subdivisions smaller than a state

3. All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical Records numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locaters (URL)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

(note this does not mean the unique code assigned by the investigator to code the data)

BREACH is defined by the HITECH Act as the unauthorized access, use of disclosure of ***unsecured* PHI** which compromises the security or privacy of the information (except where an unauthorized person would not reasonably have been able to retain such information).

- Breach may include any loss of an information device or media (such as a flash drive, laptop, Smart phone, PDA, CD/DVD etc.) which contains PHI
- Breach may also result from the unauthorized access, use, or disclosure of PHI included in clinical records (i.e.) hardcopy documentation

Breach may result from sending PHI to an incorrect email address or fax number, posting PHI on an unsecured website, or the unauthorized access of PHI from an application, database, or another individual's private account.

UNSECURED PROTECTED HEATH INFORMATION (PHI): As defined in the federal HIPAA Privacy and Security Rules at 45 CFR 402, unsecured PHI is protected health information that is **not secured by a technology standard** that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance issued in accordance with law and posted on the Health and Human Services website.

Policy Guidelines

Routine Activities

As a member of our agency staff, you routinely use protected health information about clients to carry out your duties. You may also need to disclose protected health information about clients to persons outside the agency or to request protected health information from these persons. The agency has specific policies and procedures explaining how much information may be used, disclosed or requested in situations that occur on a routine basis. You are expected to know and follow these policies at all times. These policies have been carefully developed and are not intended to limit any communications required for agency staff to provide quick, effective and high quality service. If you have any questions about how these should be applied in a particular situation, contact your supervisor.

Non-Routine Situations

Agency policies are general policies that address routine activities. If the general policies and procedures do not address a particular situation or do not permit you to use, disclose or request protected health information in a way that you believe it is necessary to carry out your duties, you should **notify your supervisor**. Your supervisor will be responsible for providing guidance or directing you to the agency staff members who can more appropriately address the situation. If necessary, your supervisor will consult with the agency's Human Resource/Corporate Compliance Manager to determine how much information may be used, disclosed or requested. Individual agency staff members should not make decisions on their own if the situation is not covered in agency policies or procedures or in their specific program's policies and procedures.

Emailing and Faxing Information

Agency staff should not transmit protected health information over the internet (including email) and other unsecured networks. Sending PHI over LAUNCH accounts is a secure system because it is a Gmail based email system. PHI can safely be transmitted among LAUNCH staff, only as necessary for service to a client, without further encryption as long as the email is sent from your LAUNCH agency email. Sending PHI to others outside of the agency is only secure if you are sending it to another Gmail account.

If you need to send information to an email that you do not know if it is secure or not, you must put the information in a word document that is password protected before sending the information. The password can be sent by email in a separate email from the password protected document.

Transmission of protected health information is permitted by fax **only** if the agency staff member is sending the information ensures that the intended recipient is available to receive the fax as it arrives, or confirms that there is a dedicated fax machine that is monitored for transmission of sensitive information. Agency staff should use LAUNCH fax cover sheets which include standard confidentiality notices, and should request that the recipient call the staff member upon receipt of the fax.

Public Viewing/hearing

Agency staff is expected to keep protected health information out of public viewing and hearing. For example, protected health information should not be left out in conference rooms, put on desks, or on counters or other areas where the information may be accessible to the public or to other employees or individuals who do not have a need to know the protected health information. Agency staff should also refrain from discussing protected health information in public areas, such as elevators or reception areas, unless doing so is necessary to provide service to a client. Agency staff should also take care in sharing protected health information with families and friends of clients. Such information may generally only be shared with a consumer's **"personal representative"** or to a client's family, relative or close personal friend who is involved in the client's care or payment for the client's care. Even in the latter circumstance, information cannot be disclosed unless the client has had a chance to agree or object to the disclosure, and you may only disclose information that is relevant to the involvement of that family member, relative or close personal friend in the client's care or payment for the client's care, as the case may be.

Databases and Workshops

Agency staff is expected to ensure that they exit any confidential database upon leaving their work stations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. Agency staff are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including, but not limited to, any password, personal identification number, token or access card, or electronic signature. Each agency staff member will be liable for all activity occurring under his or her account, password and/or electronic signature. These activities may be monitored.

Downloading, Copying or Removing

Agency staff should not download copy or remove from the agency any protected health information, except as necessary to perform their duties at the agency. Upon

termination of employment or contract with the agency, or upon termination of authorization to access protected health information, agency staff members must return to the agency any and all copies of protected health information in their possession or under their control.

Computers and Media Security
All employees must read and understand their responsibilities regarding use of portable computing and media devices in terms of privacy and security of confidential information. All employees are also required to sign a Privacy and Security Agreement which will be retained in their Human Resources file.

Breach of unsecured PHI
These requirements are under the Breach Notification Rule, section 13402 of Title XIII of the Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act of 2009.
These procedures implement the actions required to:

- **Report and identify** unauthorized disclosures of unsecured Protected Health Information (PHI)
- **Assess the risk** posed by such disclosures and determine whether a breach occurred and if so;
- **Timely notify** individual(s) of the breach

Suspected breach: Any staff member or associate who suspects a breach is to report this to his or her supervisor, who will bring this to the Associate Executive Director. The Executive Director will make a determination regarding the breach in concert with the Associate Executive Director and the Privacy and Security Officer.

The following information needs to be gathered to **complete a report** and conduct an investigation of the suspected breach:

- Date of the suspected breach
- Description of what happened, including type of media involved, e.g. flash drive, CD/DVD, email, paper documents;
- Description of the type of unsecured protected health information that was involved in the suspected breach;
- Number of individuals whose information was disclosed or the scope of the suspected breach;
- Description of actions taken to investigate the breach; and
- Description of the actions taken to mitigate the breach

Breach Determination and Notification Process

(1) Upon receiving a report of a suspected breach incident, Associate Executive Director, Executive Director and Privacy and Security Officer will review the report to determine whether there has been unauthorized access, use or disclosure of unsecured PHI by LAUNCH staff or others in violation of the HIPAA Privacy or Security Rule.

(2) If the incident results in unauthorized access, use or disclosure of unsecured PHI, the Associate Executive Director, Executive Director and Privacy and Security Officer will determine whether the incident poses a "significant risk of harm" to the individual(s) using a Risk Assessment Tool. This document is retained along with other documentation related to the suspected breach.

Factors considered in the risk assessment determination include:

- What type of PHI was disclosed?
- What amount of PHI was disclosed as a result of the incident?
- Who used or had access to the disclosed information? Was it disclosure to another covered entity?
- Was the unauthorized disclosed PHI returned before it could be accessed and used?
- What immediate steps were taken to mitigate the risks associated with the unauthorized use or disclosure?
-

(2) If it is determined that the incident poses a significant risk of harm to the individual(s), the Associate Executive Director, Executive Director and Privacy and Security Officer will determine whether the incident

(3) qualifies as an **exception from a breach**, including:

- Good faith, unintentional acquisition, access or use of PHI by a LAUNCH staff member that does not result in further unauthorized use or disclosure in violation of the HIPAA Privacy Rule.
- Inadvertent disclosure by an individual authorized to access the PHI to another individual authorized to access the PHI, provided that the disclosure does not result in further unauthorized use of disclosure; or
- Disclosures where LAUNCH has determined that the unauthorized recipient would not have reasonably been able to retain the disclosed information (example: documents including PHI are mailed to the wrong individuals but they are returned undeliverable and unopened; staff person opens a file containing PHI on the laptop in the presence of others, but closes the laptop before it can be read by anyone).

(4) If it is determined that the incident poses a significant risk of harm to the individual(s) and **no exceptions to the definition of breach applies**, the incident is determined to be a breach. LAUNCH Executive Director will assure the required notifications are made.

LAUNCH will notify each individual whose unsecured PHI was breached. LAUNCH will notify such individuals without reasonable delay and in no case, later than 60 calendar days following the discovery of the breach by LAUNCH. Breach notifications will include the following information:

- A brief description of the incident, including the date of the breach and the date the breach was discovered, if known;
- A description of the types of unsecured PHI that was breached;
- Steps that the individual should take to protect themselves from harm resulting from the breach;
- A brief description of the actions taken by LAUNCH to investigate the breach, mitigate the risk of harm to the individual(s) resulting from the breach, and steps taken to protect individuals from future breaches and;
- Contact information for individuals to ask questions or gather additional information, including as appropriate, telephone numbers, e-mail addresses, websites and postal addresses.

Notifications

LAUNCH will provide written notice to **Individuals:**

- By first class mail to the last known address of each individual; or
- By electronic mail, if the individual agrees to receive electronic notices, and such agreement has not been withdrawn; or
- By hand delivery

If the affected individual is a minor or otherwise lacks legal capacity, the notification will be sent to the individual's personal representative. If the person is deceased, the notice may be sent to the individual's next of kin or personal representative, if known.

Secretary of the US Department of Health & Human Services (HHS):

LAUNCH will notify the Secretary of HHS of all breaches of unsecured PHI on an annual basis. LAUNCH will submit such breaches to HHS within 60 days of the end of each calendar year in accordance with instructions posted on the HHS website.

Breaches involving more than 500 individuals: LAUNCH will make notifications to individuals and HHS following protocols on the HHS website.

Documentation
LAUNCH Privacy and Security Officer will maintain a log of all notifications of breaches involving less than 500 individuals. The Privacy and Security Officer will also retain records and documentation related to breach reports, investigations, determinations and notifications.

Business Associate Agreement
In addition to routine contracts for specific services (such as cleaning services and information technology), Business Associates, as defined in the HIPAA Final Omnibus Rule, will be required to review, understand and sign an Agreement with LAUNCH which clarifies responsibilities regarding privacy and security of confidential information. This agreement also clarifies the process if the Business Associate has a breach of privacy and/or security, and the process to follow when a Business Associate contractual arrangement is terminated.

Training
LAUNCH staff will be trained on the HIPAA Privacy and Security Rules, as well as on the HITECH Breach Notification Rule "as necessary and appropriate for them to carry their function within LAUNCH.

Training will be provided for all staff and will be part of new staff orientation. A periodic refresher will be provided as an annual update.

Violations
The agency's Executive Director has general responsibility for implementation of this policy. Members of the agency staff who violate this policy will be subject to disciplinary action up to and including termination of employment or contract with LAUNCH. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the agency's Executive Director or Privacy and Security Officer. All reported matters will be investigated, and where appropriate, steps will be taken to remedy situation. Where possible, LAUNCH will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with LAUNCH.

LAUNCH's Privacy and Security Officer: Amy Eells amy.eells@accesscny.org or 315-410-3318

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Compliance Investigations **June 2023**
Policy 510

Policy:

LAUNCH will ensure that all Corporate Compliance complaints are addressed in a thorough and timely manner. Corporate Compliance complaints may include, but are not limited to the following:

- submitting or signing a report or billing for service not rendered
- falsifying or altering documentation
- omitting required documentation or failing to timely complete required documentation
- misappropriation of agency or participant funds
- illegal actions/activities

To the greatest extent possible, an investigation of Corporate Compliance issues will remain confidential, although the nature of some investigations makes certain disclosures unavoidable.

Procedure:

1. All complaints will be reported a supervisor or to the Compliance Officer. The complaint can be reported verbally, in written form or through the Hot Line. LAUNCH's Compliance Hot Line number is **(315)410-3333.** Complaints may be reported anonymously. If a report is made by an employee to his/her supervisor, the supervisor receiving the complaint will report the complaint to the Compliance Officer.

2. The Compliance Officer will check the Hot Line number on a regular basis. The Compliance Officer will assign a designated person to receive complaints and check the Hot Line in the event that the Compliance Officer will be away from the office for more than two business days.

3. All the compliance complaints received will be documented with the action taken by the Compliance Officer on the compliance tracking sheet.

4. Upon receipt of a complaint, the Compliance Officer will determine whether the complaint warrants an investigation. A full investigation will be completed for all concerns of potential fraud. If the concern reported is clear that it's due to an unintentional error, the Compliance Officer will discuss appropriate follow-up with appropriate management staff. If the complaint does not warrant an investigation or is not related to Corporate Compliance, the Compliance Officer will forward the complaint to the appropriate management staff. In the event that an investigator is not available, the Compliance Officer will conduct the investigation.

5. The Compliance Officer will notify the Executive Director and Associate Executive Director.

6. In the event that it is determined that the employee involved should be suspended without pay during the investigation, the Associate Executive Director or designee who oversees the employee will notify the employee.

7. The assigned investigator will initiate an investigation within two business days of receipt of the complaint.

8. The investigator will conduct interviews, review documentation and complete a written investigation report with findings, conclusion and recommendations.

9. The Compliance Officer will review the investigation report and forward the conclusion and recommendations to the Executive Director and the Associate Executive Director within ten business days of the complaint. If the investigator requires more time, the Corporate Compliance Officer will forward the status of the investigation to the Executive Director, and Associate Executive Director.

10. If disciplinary action is recommended, the investigator will schedule a meeting with the Compliance Officer, Executive Director and Associate Executive Director to discuss the findings and decide on disciplinary follow-up. If it is determined that the complaint was not reported in good faith, but was done with malice, follow-up will occur with the employee and disciplinary action may be taken against the person filing the initial complaint.

11. The Associate Executive Director will forward results of actions taken by the agency regarding the complaint to the Compliance Officer within 30 days of receipt of the written report. Actions may include disciplinary action and/or termination of the employee involved, re-training, police involvement or self-disclosure to outside overseeing agencies.

12. If requested by the initiating employee, the Compliance Officer will respond to the person initiating the complaint (if disclosed) within 15 business days regarding the activities in process. (The details or findings of the investigation will not be disclosed to the complainant).

13. The Compliance Officer will ensure that all complaints and investigations are kept secure for 10 years. All documentation is stored electronically and securely on SharePoint.

14. The Compliance Officer will review the investigation and actions taken by the agency with the Compliance Committee on a quarterly basis. Any additional recommendations made by the Committee will be forwarded to the applicable management staff.

15. The Compliance Officer will submit a quarterly written report to the Audit and Finance Committee of the Board regarding Corporate Compliance complaints and investigations. Agency trends will also be shared on an annual basis with the Board of Directors.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Compliance Training and Education Plan **June 2023**
Policy 511

LAUNCH is committed to ensuring that all affected individuals receive the necessary training to ensure knowledge of LAUNCH's compliance requirements and expectations. This will be carried out by the following:

Employees

- All new employees receive compliance training within 30 days of date of hire. This includes program specific information on risk areas for those working in Medicaid funded programs. This training takes place during new hire orientation and is also available through the online learning management system. All employees will take a post test to ensure understanding of the information. Attendance for this is tracked within Litmos.
- Compliance elements are reviewed as part of the new employee orientation checklist. A copy of this checklist can be found in each employee's ADP file.
- All staff are required to complete annual training. This includes program specific information on risk areas for staff working in Medicaid funded programs. Staff will take a pre and post test to analyze the effectiveness of the training. Attendance for this is tracked within the online learning management system, Litmos.
- An annual compliance update is provided to the Management Team annually.
- Members of the AccessCNY Quality Enhancement Team may attend LAUNCH staff meetings and discuss compliance topics as needed.
- The Compliance Officer sends monthly emails to the LAUNCH Executive and Associate Executive Directors and provides compliance topics for discussion with management team and individual teams.
- New compliance requirements are shared with management of those program areas and reviewed during regular program compliance meetings.

Board of Directors

- All new members receive training within 30 days.
- Annual compliance training is provided by the Compliance Officer.

Compliance Officer

- The Compliance Officer will participate in a minimum of 10 additional hours of compliance training and education each calendar year. This will be tracked in their training file.

Other Affected Individuals

- All other affected individuals (as identified in the compliance plan) receive information on LAUNCH's compliance plan and policies at the start of any contract. This will include information on compliance issues, expectations and the compliance program operation. They are required to acknowledge receipt of this information and this will be tracked by the Executive Director or their designee.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Exclusion Screening
Policy 512

June 2023

Policy:
LAUNCH will ensure compliance with all federal and state laws and regulations regarding exclusion screening. LAUNCH will not employ, contract with or conduct business with an individual or entity excluded from LAUNCH in state or federally sponsored health care programs such as Medicare and Medicaid.

Procedure for Employees, Consultants, Vendors/contractors and Board of Directors:

1. LAUNCH administrative assistant runs exclusion screenings for the agency. Exclusion screenings are completed prior to hire and on a monthly basis. The Administrative Assistant runs names through the required databases:
    - HHS Office of Inspector General https://apps.omig.ny.gov/exclusions/ex_search.aspx
    - Excluded Parties List System https://sam.gov/content/exclusions
    - NY Office of Medicaid inspector General https://exclusions.oig.hhs.gov/

2. The Executive Director or their designee will enter each prospective employee/consultant name into the exclusion database prior to hiring an individual.

3. If a prospective employee, consultant, vendor/contractor or board member's name shows up on any of the exclusion lists, LAUNCH will verify the information matches the prospective employee/consultant/vendor/board member. The Executive Director or their designee will notify the Corporate Compliance officer to verify the findings. If the information is a match, the employee/consultant will be ineligible for hire and the Executive Director or their designee will notify the prospective employee/consultant and the hiring manager.

4. Monthly, upon completion of the exclusion checks, the Administrative Assistant will print the results for each individual or business checked and give that information to the Executive Director. The Executive Director will review the results and file the documents. If a current employee/consultant shows up on any of the exclusion lists during a monthly screening and the information confirms the employee/consultant's identification to be a match, The Executive Director will notify the Corporate Compliance Officer to verify the findings. If

verified, the Executive Director or their designee and Program Supervisor will terminate the employee/consultant and notify LAUNCH's Compliance Officer. The Compliance Officer will follow the Self-Disclosure standard as it relates to this compliance concern.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

False Claims Act **June 2023**
Policy 513

Policy:
LAUNCH and its employees and all affected individuals shall not make or submit any false or misleading entries on any claim forms. No employee or affected individual shall participate, direct, or assist another person to submit a false or misleading entry on claims or documentation of services that result in the submission of a false claim.

Overview of the Federal False Claims Act

The False Claims Act, 31 U.S.C. 3729 *et seq.,* is a federal law designed to prevent and detect fraud, waste and abuse in federal healthcare programs, including Medicaid and Medicare. Under the False Claims Act, anyone who "knowingly" submits false claims to the Government is liable for damages up to three times the amount of the erroneous payment plus mandatory penalties of $10,000 - $50,000 for each false claim submitted.

- The definition of "knowingly" includes a person who:
- Has actual knowledge of falsity of information in the claim
- Acts in deliberate ignorance of the truth or falsity of the information in the claim
- Acts in reckless disregard of the truth or falsity of the information in the claim

Whistleblower or "Qui Tam" Provisions

In order to encourage individuals to come forward and report misconduct involving false claims, the False Claims Act contains a "Qui Tam" or whistleblower provision.

The Government, or an individual citizen acting on behalf of the Government can bring actions under the False Claims Act. The individual taking action, "whistleblower" and has information regarding the false claims may file a lawsuit on behalf of the U.S. Government. If the lawsuit is successful, and provided certain legal requirements are met, the whistleblower may receive an award ranging from 15% - 30% of the amount recovered.

The False Claims Act provides provisions which prohibit discrimination by LAUNCH against any employee, former employee, contractor or agent for taking lawful actions.

Please refer to the Whistleblower Policy (Policy #517)for more information.

New York State False Claims Act:

The State False Claims Act is very similar to the Federal False Claims Act. It also imposes fines and penalties on individuals and agencies that file false and fraudulent claims for payment from any state or local government, including health care programs such as Medicaid. The New York State False Claims Act also includes similar whistleblower provisions.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Identification of Compliance Risk Areas **June 2023**
Policy 514

Policy:
LAUNCH will develop and implement a system to assess and minimize the risk of each program of the agency.

Procedure:

1. Each year the Corporate Compliance Officer will review and update the risk assessment survey according to regulation updates and trends.

2. At the end of each year, the Compliance Officer will forward the agency's risk assessment survey to each department's Program Director or designee for completion.

3. The completed risk assessments will be reviewed by the Compliance Officer and the results tallied by a number system.

4. The Compliance Officer will present the tallied results to the Compliance Committee and each program will be ranked low risk, moderate risk or high risk.

5. The results and recommendations from the Committee's review of the risk assessments will be included in the LAUNCH's annual compliance work plan.

6. Each high risk program will create a work plan to address their identified areas of risk. The Compliance Officer will work with each program to reduce the identified risk by reviewing the work plan status at program compliance meetings.

7. The Compliance Officer will review the status and progress of the agency annual work plan at the Compliance Committee meetings.

8. The Compliance Officer will review LAUNCH's Compliance work plan with the Board of Directors on an annual basis and as the need arises.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Self-Disclosures **June 2023**
515

Policy:
LAUNCH is committed to ensuring that the agency's documentation, coding and billing practices comply with all federal and state laws and regulations. LAUNCH prohibits the intentional submission for reimbursement of any claim that is false, fraudulent or fictitious.

At times, LAUNCH may receive an overpayment for services. *When the overpayment is considered a minor error, LAUNCH will return the overpayment through the process of adjusting or voiding the claim. When it is determined that the overpayment is more significant, LAUNCH will self-disclose the overpayment to the Office of the Medicaid Inspector General. Issues appropriate for disclosure may include, but are not limited to:

- Substantial routine errors
- Systemic errors
- Patterns of errors
- Potential violation of fraud and abuse laws

**LAUNCH will follow any updated guidance OMIG releases specific to disclosure.*

Procedure:

1. Each department will develop a billing procedure which will include a process to ensure that all required documentation is present prior to billing for services. The supervisor should ensure that the Finance department does not submit billing claims without verification that the required documentation is present.
2. The Finance department will keep a record of billing claims that they have discovered or have been directed to adjust or void after the claim has been billed. These will be reported to the compliance officer via approved form.
3. The Compliance Officer will review all identified overpayments with the Compliance Committee.
4. The AccessCNYQuality Enhancement department will conduct a random sample of billing claims for each Medicaid program as part of the monthly pre-billing audits. If any billing concerns or discrepancies are discovered, this information will be documented in the audit report and the department will need to correct the discrepancies prior to billing submission. *Please refer to Medicaid pre-billing audit standard and procedure #1501 and #1502.*

5. Whenever an error becomes significant or fraud is substantiated through the investigation process, the Compliance Officer will notify the Executive Director to determine whether LAUNCH's attorney should be consulted.
6. The Compliance Officer will submit a quarterly report to the Audit and Finance Committee of the Board regarding billing issues and self-disclosures. This will be a written report unless otherwise requested. The Compliance Officer will meet with the Board of Directions annually in-person.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Subpoena and Search Warrant **June 2023**
516

Policy:
LAUNCH will comply fully with any lawful subpoena or search warrant.
LAUNCH employees will remain courteous and professional when dealing with investigators or agents delivering a subpoena or executing a search warrant.

Procedure:

Subpoena

1. If a subpoena is received, either in person or via the mail, it must be immediately provided to the Executive Director who will contact the Associate Executive Director of Quality & Performance at AccessCNY.

2. If delivered in person, the recipient shall obtain further information (e.g., the name, title, and telephone number of the serving agent/investigator and information provided by the agent/investigator).

3. Employees shall not volunteer information to an agent/investigator or submit to any form of questioning or interviewing without direction from legal counsel.

4. The Executive Director will identify the individual at the facility who is most qualified and available to assist legal counsel in responding to the subpoena.

Subpoena (Employee Related)

1. When a subpoena is received for Personnel File Information either in person or via mail, the Executive Director shall be notified first. In the absence of the Executive Director, the Associate Executive Director shall be notified. If a subpoena is received via mail, it shall be reviewed by the Executive Director or Associate Executive Director, in the absence of the Executive Director, before the subpoenaed information is provided.

2. If delivered in person, the recipient shall obtain further information (e.g., the name, title and telephone number of the serving agent/investigator and information provided by the agent/investigator).

3. The Executive Director or Associate Executive Director shall not volunteer information to the agent/investigator regarding the subpoena or submit to any form of questioning or interviewing without direction from legal counsel.

4. A processing check for $15.00 is sometimes received with the subpoena. This check shall be forwarded to the Executive Director. The check will not be deposited until the response to the subpoena has been provided to the requesting entity.

Search Warrant

1. If a federal or state law enforcement agency arrives at LAUNCH with a search warrant, the employee greeting the agent shall ask for identification and immediately contact the Executive Director or the Associate Executive Director, in the absence of the Executive Director.

2. The Executive Director or Associate Executive Director, and if necessary, shall contact outside legal counsel and follow legal counsel's direction.

3. Before the agent executes the search warrant, the Executive Director or Associate Executive Director shall view and photocopy the search warrant document. Carefully examine the search warrant (with legal counsel, if possible) to determine the following:
    - Determine the specific areas or locations it covers;
    - Ensure that it is being executed during the hours indicated on the document (most warrants should limit the hours they can be executed, e.g. "daylight hours);
    - Ensure that it has not expired (all warrants have an expiration date);
    - Ensure that it is signed by a Judge (all warrants should be signed by a Judge).

4. Politely object if any overt flaw in the warrant is apparent or if the agents are searching for anything you deem to be outside the scope of the warrant. Do not interfere should agents proceed and search. Note the fact for legal counsel to support a future protest.

5. The Executive Director, Associate Executive Director, shall request an "inventory list" of the documents and items seized by the agents. A separate record of the areas searched, and items seized shall be maintained.

6. Other than providing information to direct the agents to information requested, LAUNCH employees shall not submit to any form of questioning or interviewing without the direction of legal counsel.

7. The Executive Director or Associate Executive Director will go to the site as soon as possible and remain present while the agents are conducting the search. However, program staff are not to prevent the search from happening prior to their arrival.

LAUNCH, a New York not-for-profit Agency (the "Agency"), requires its directors, officers, employees, key persons, contractors and volunteers to observe high standards of business and personal ethics in the conduct of their duties and responsibilities within and on behalf of the Agency. As representatives and employees of the Agency, you must comply with all applicable laws and regulations and act with honesty and integrity in fulfilling your responsibilities.

The purpose of this Whistleblower Policy ("Policy") is to ensure that the Agency has a governance and accountability structure that supports its mission, to encourage and enable directors, officers, employees, key persons, contractors and volunteers of the Agency to raise serious concerns about the occurrence of illegal, fraudulent or unethical actions within the Agency, and to protect those individual who report from retaliation.

Notwithstanding anything contained in this Policy, this Policy is not an employment contract and does not modify the employment relationship, if any, between the Agency and any of its directors, officers, employees, key persons, contractors or volunteers, nor does it change the at-will status of any employee of the Agency. Nothing contained in this Policy provides any director, officer, employee, key person, contractor or volunteer of the Agency with any additional rights or causes of action not otherwise available under applicable law.

It is intended that this Policy complies with the provisions of Section 715-B of the New York State Not-for-Profit Agency Law, as added by the Non-Profit Revitalization Act of 2013, as amended, and shall be interpreted and construed accordingly. This Policy applies to any matter which is related to the Agency's business and does not relate to the private acts of an individual not connected to the business of the Agency. The rights and protections set forth in this Policy are in addition to, and not in abrogation of, the protections provided by Sections 740 and 741 of the New York State Labor Law, Section 191 of the New York State Finance Law or any applicable Federal law, including but not limited to the False Claims Act (31 USC § 3730(h)).

ARTICLE I
REPORTING RESPONSIBILITY

1.1 Reporting Responsibility. All directors, officers, employees, key persons and volunteers of the Agency have a responsibility to report any action or suspected action taken by the Agency itself, by its leadership or by others on the Agency's behalf, that is illegal, fraudulent, unethical or violates any adopted policy of the Agency ("Violations").

1.2 Reporting in Good Faith. Anyone reporting a Violation must act in good faith, without malice to the Agency or any individual and have reasonable grounds for believing that the information shared in the report indicates that a Violation has occurred. A person who makes a

report does not have to prove that a Violation has occurred. However, any report which the reporter has made maliciously or any report which the reporter has good reason to believe is false will be viewed as a serious disciplinary offense.

ARTICLE II
NO RETALIATION

2.1 No Retaliation. No person who in good faith reports a Violation or who in good faith cooperates in the investigation of a Violation shall suffer intimidation, harassment, discrimination or other retaliation or, in the case of employees, any adverse employment consequence. Any individual within the Agency who retaliates against another individual who has reported a Violation in good faith or who, in good faith, has cooperated in the investigation of a Violation shall be subject to discipline, including, without limitation, termination of employment or volunteer status.

2.2 Reporting of Retaliation. If you believe that an individual who has made a good faith report of a Violation or who has in good faith cooperated in the investigation of a Violation is suffering intimidation, harassment, discrimination or other retaliation or, in the case of employees, adverse employment consequence, you should make a report to the Corporate Compliance Officer. *Please refer to the Non-Intimidation and Retaliation Policy (Policy 520).*

ARTICLE III
PROCEDURES FOR REPORTING VIOLATIONS

3.1 Reporting Procedure. All directors, officers, employees and volunteers should address their concerns relating to a Violation to any person within the Agency who can properly address those concerns. In most cases, the direct supervisor of an employee or volunteer is the person best suited to address a concern. However, if you are not comfortable speaking with your supervisor or if you are not satisfied with your supervisor's response, you are encouraged to speak to the Corporate Compliance Officer, to any member of the Governance and Compliance Committee of the Board of Directors of the Agency (the "Board") or to anyone in management you feel comfortable approaching. If a direct supervisor or other person receives a report of a concern, that information should be shared with the Compliance Officer. If you are not an employee or volunteer, you should report any Violation directly to the Corporate Compliance Officer. If you are not comfortable making a report to the Compliance Officer or if the Compliance Officer is the subject of the complaint, a report can be made directly to a member of the Audit and Finance Committee of the Board or the Executive Director.

3.2 Identity; Confidentiality. The Agency encourages anyone reporting a Violation to identify themselves when making a report to facilitate the investigation of the Violation. However, reports addressed to an individual within the Agency may be submitted on a confidential basis and reports may be submitted to the Corporate Compliance Officer anonymously by submitting them directly, without providing an identity or return address, to the Corporate Compliance Officer using the contact information set forth in **Section 5.2** below.

3.3 How to Report. The report of any Violation may be made in person, by telephone or by mail, electronic mail or other written communication. The report should contain sufficient information to permit adequate investigation. At a minimum, the following information should be provided: (a) a description of the nature of the improper activity, with sufficient detail to permit an initial investigation; (b) the name(s) of the individual(s) and/or department(s) engaging in the activity

or with knowledge of the activity; (c) the approximate or actual date(s) the activity took place; and (d) an explanation of any steps taken internally with the Agency's management to report or resolve the complaint.

ARTICLE IV
COMPLIANCE AND ADMINISTRATION

4.1 Notification of Violation; Acknowledgement. Every supervisor, manager, director and other representative of the Agency is required to notify the Corporate Compliance Officer of every report of a Violation. The Corporate Compliance Officer will notify the sender and acknowledge receipt of a report of Violation within seven (7) business days, but only to the extent the sender's identity is disclosed or a return address is provided.

4.2 Investigation; Correction.

(a) The Corporate Compliance Officer is responsible for promptly investigating all reported Violations and for causing appropriate corrective action to be taken if warranted by the investigation. The Corporate Compliance Officer shall conduct an investigation into the reported Violation as soon as practicable thereafter. Such investigation shall be conducted as confidentially as possible under the circumstances, consistent with the need to conduct an adequate investigation, to comply with all applicable laws, and if appropriate, to cooperate with law enforcement authorities.

(b) The Corporate Compliance Officer shall review the policies and procedures of the Agency and make note of any alleged Violation. A log should be maintained of all Alleged Violations and the results of the investigation.

(c) The Corporate Compliance Officer shall assess, in the most confidential manner possible, the concerns of the director, officer, employee, key person or volunteer who reported the alleged Violation, as well as those of other directors, officers, employees or volunteers who may have an understanding of, or be complicit in, the alleged Violation, in order to form an informative opinion on the matter and determine potential recommendations for resolution.

(d) The Corporate Compliance Officer may contact the Agency's counsel, as needed, during an investigation of a reported Violation.

(e) The Corporate Compliance Officer will prepare and submit a written report on the reported Violation to the Board of the Agency, together with recommendations as to resolution and a timeline for implementation of recommended actions. The Corporate Compliance Officer will also forward a copy of the written report to the Board.

(f) The Board shall act on the Corporate Compliance Officer's written report as appropriate, including reviewing all findings and recommendations identified therein, and submitting a written assessment of the matter, including recommendations as to resolution and a timeline for implementation of recommended actions, to the Board.

(g) Upon receipt of the written report from the Board, the matter will be considered binding and any action items, up to and including, the suspension or removal of any director, officer, employee, key person or volunteer found to have engaged in the reported Violation will be effectuated as soon as practicable.

(h) In the event that the Compliance Officer is the subject of a complaint, The Governance and Compliance Committee of the Board will assume all responsibilities of the investigation as identified above.

4.3 Administration.

(a) The Corporate Compliance Officer shall administer this Policy and shall report directly to the Board.

(b) Any person who is the subject of a whistleblower complaint shall not be present at or participate in Board deliberations or vote on the matter relating to such complaint; provided, however, that the Board may require that the person who is subject to the complaint present cooperate in the investigation and provide information or answer questions at the Board meeting prior to the commencement of deliberations or voting relating thereto.

(c) The Board is responsible for addressing all reported concerns or complaints of Violations relating to corporate accounting practices, internal controls or auditing. Accordingly, the Corporate Compliance Officer must immediately notify the Board of any such concern or complaint. In addition, if the Corporate Compliance Officer deems it appropriate, the Corporate Compliance Officer may advise the chair of the Board of any other reported Violations.

4.4 Reporting. The Corporate Compliance Officer has direct access to the Board and is required to report to it at least quarterly on compliance activity.

4.5 Documentation. The Board shall assure that all reported Violations and investigations are properly documented, including minutes of any meeting of any Committee or the Board where the matter was discussed. The documentation shall be maintained for a period of at least 10 years or longer in the event any investigation, audit or other inquiry is pending relating thereto.

ARTICLE V
MISCELLANEOUS

5.1 Access to Policy. A copy of this Policy shall be distributed to all directors, officers, employees, key persons and volunteers who provide substantial services to the Agency and available on the website and the agency's SharePoint site.

5.2 Corporate Compliance Officer. The contact information of the Corporate Compliance Officer is as follows:

Amy Eells, Associate Executive Director of Quality and Performance
6666 Manlius Center Rd.
East Syracuse, NY 13057
(315)410-3318
amy.eells@LAUNCH.org

5.3 Modification. The Agency may modify this Policy unilaterally at any time without notice. Modification may be necessary, among other reasons, to maintain compliance with federal, state or local laws and regulations and/or to accommodate organizational changes within the Agency.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Standards of Conduct **June 2023**
Policy 518

Standard:
LAUNCH employees and affected individuals will maintain the highest standards of ethical conduct and compliance with all applicable Federal and State laws and regulations as well as LAUNCH's Guiding Principles located in the HR Policy 103.

Procedure:

- LAUNCH employees and affected individuals will adhere to the agency's guiding principles as provided in HR Policy 103.

- LAUNCH employees and affected individuals will provide quality care in the most appropriate setting that is necessary, verifiable and respects the rights and dignity of the individual.

- LAUNCH employees and affected individuals will comply with all applicable laws, regulations, standards and requirements.

- LAUNCH employees and affected individuals will not pursue any business opportunity that requires engaging in unethical or illegal activity.

- LAUNCH employees and affected individuals will maintain accurate and complete records of all services provided with proper documentation as required by regulatory agencies.

- LAUNCH employees and affected individuals will submit claims and billing statements in a timely manner that accurately reflect rendered services. LAUNCH employees and affected individuals will not submit false, fraudulent or fictitious claims.

- LAUNCH will provide a mechanism for anyone to report compliance concerns and a process to investigate issues. LAUNCH employees and affected individuals are expected to participate in an initial and annual Corporate Compliance training. LAUNCH employees and affected individuals are expected to report any unethical, illegal or fraudulent incidents to the Corporate Compliance Officer in a timely manner without fear of reprisal in accordance with the agency's Whistleblower policy #517.

- LAUNCH will ensure compliance with regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). LAUNCH shall maintain the highest degree of confidentiality regarding participants, personnel, and business information consistent with the law.

- LAUNCH will only employ persons with proper credentials, experience and expertise.

- LAUNCH values diversity and will not discriminate in any matter based on ethnic background, disability, national origin, sex, age, marital status, sexual orientation or any other protected category.

- LAUNCH employees and affected individuals should avoid any activity that conflicts with the interests of the agency.

- In accordance with the Anti-kickback Statute:
    a) LAUNCH employees and affected individuals will not accept or provide benefits that could be seen as creating conflict between their personal interests and the agency's legitimate business interests. This includes accepting expensive meals, gifts, refreshments or entertainment.
    b) Any contributions or donations will be obtained without coercion, force or expectation of compensation in return.
    c) LAUNCH employees or affected individuals will not pay employees, physicians, or other health care professionals, directly or indirectly, in cash or by any other means, for referral of patients. Every payment to a referral source must also be supported by proper documentation.

- LAUNCH employees and affected individuals are responsible and accountable for proper expenditure of the agency's funds and for the proper use of agency property.

- Any improper financial gain to the employee through misconduct involving misuse of the agency's or participants' funds or property is prohibited.

- LAUNCH shall prepare and maintain accurate and complete cost reports, financial records and statements regarding the agency's assets, liabilities, revenue and expenditures, according to generally accepted accounting principles.

- LAUNCH employees who violate the agency's Code of Ethical Conduct may receive disciplinary action, up to and including termination.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Unannounced Visit by Auditor or Investigator **June 2023**
519

Standard:
LAUNCH is committed to appropriately responding and not interfering with any lawful audit, inquiries or investigations. LAUNCH employees shall respond and cooperate with official requests for information by a government investigator or auditor.

Procedure:

1. Announcement of an impending visit by any government investigator or auditor related to **billing** should be immediately reported to the Executive Director, Associate Executive Director of Quality & Performance at AccessCNY. This would include any visits by the Office of Medicaid Inspector General (OMIG) and the Office of Inspector General (OIG) and may include the Office of People With Developmental Disabilities (OPWDD) and AccesVR

2 If there is an unannounced visit by a government investigator, auditor or other representative at any site operated by LAUNCH, the employee greeting the investigator or auditor should treat him or her with respect and courtesy. The employee shall request identification and the reason for the visit.

3 The employee shall contact the Program Director immediately and inform the Program Director of the investigator/auditor's name, agency and purpose of the visit. The investigator/auditor shall be asked to wait in an unused office or location where business is not conducted until a management staff arrives.

4 The Program Director shall immediately contact the Executive Director and Associate Executive Director and they will contact the Associate Executive Director of Quality & Performance at AccessCNY.

5 The Executive Director shall appoint someone to be the primary contact person with the investigator/auditor. In most situations, the Associate Executive Director shall be appointed the primary contact person.

6 The primary contact person shall meet directly with the investigator/auditor and document the information requested. The primary contact person shall obtain information and documents requested by the investigator/auditor. No documentation should be given to the investigator/auditor until the appointed primary contact person has met with the investigator/auditor. LAUNCH's legal counsel should be consulted if there are any questions before information and documentation is given to the investigator/auditor.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Non-Retaliation and Non-Intimidation Policy **June 2023**
Policy 520

PURPOSE

The purpose of this Policy is to ensure that employees, Board of Directors ("Board") members, and contractors of LAUNCH are encouraged to report concerns about the occurrence of serious illegal, fraudulent or unethical actions within the organization ("Compliance Issues"). "Compliance Issues" are actual or suspected fraud, waste, abuse, other wrongful or unethical conduct, or violations of laws, regulations, administrative guidance, or LAUNCH's Compliance Plan[1] and policies. Employees, Board members, and contractors are protected from intimidation and retaliation for good faith participation in LAUNCH's Compliance Program, including but not limited to reporting Compliance Issues, investigating issues, conducting self-evaluations, audits, and remedial actions, and reporting to appropriate officials.

APPLICABILITY

This Policy applies to all LAUNCH employees, Board members, and contractors.[2]

POLICY

1. LAUNCH prohibits any act of retribution, discrimination, harassment, retaliation, or intimidation against any employee, Board member, or contractor who, in good faith, participates in LAUNCH's Compliance Program activities, including, but not limited to:
    a. Reporting and responding to potential Compliance Issues to appropriate personnel;
    b. Participating in investigation of, and investigating, potential Compliance Issues;
    c. Conducting or responding to audits, investigations, reviews, or compliance self-evaluations;
    d. Drafting, implementing, or monitoring remedial actions;
    e. Reporting compliance-related concerns to any government entity;
    f. Attending or performing compliance-related training;
    g. Reporting instances of intimidation or retaliation; or

[1] LAUNCH's Corporate Compliance Plan ("Compliance Plan") is the document that provides an overview of LAUNCH's Corporate Compliance Program ("Compliance Program"). The Program is LAUNCH's implementation of the Compliance Plan and includes all of LAUNCH's compliance activities.

[2] "Employees, contractors, and Board members" includes LAUNCH's employees, Chief Executive Officer ("CEO"), senior administrators, managers, contractors, agents, subcontractors, independent contractors, corporate officers, and Board members who are affected by LAUNCH's Compliance Risk Areas. "Compliance Risk Areas" are those areas of operation-affected byLAUNCH's Compliance Program, as set forth in its Compliance Plan.

h. Otherwise assisting in any activity or proceeding regarding any Compliance Issue.

2. A good faith report means one where the individual believes the information reported to be true and where the report is not made for the purpose of harming the standing or reputation of LAUNCH, or of another employee, Board member, or contractor.

3. The protections of this Policy do **not** apply to:
   a. Intentional untruthful allegations of wrongdoing;
   b. Allegations whose nature or frequency indicate an intent to harass or embarrass LAUNCH or any employees, Board members, or contractors; or
   c. Instances where individuals report their own lapses or complicity in unacceptable conduct. In such instances, the act of reporting will not be subject to sanctions, but the underlying conduct may be subject to disciplinary action.

PROCEDURE

1. Reporting Mechanisms.

Employees, Board members, and contractors have a duty to report actions that they believe in good faith to be an actual or suspected Compliance Issue. *See Self Disclosure Policy (Policy #515)* Employees, Board members, and contractors have a variety of reporting options; however, they are encouraged to take advantage of internal reporting mechanisms. These include reports to the Corporate Compliance Officer or Compliance Committee member, LAUNCH's Compliance Hotline or in the case of an employee, reports to the employee's supervisor or any supervisor.

2. Reporting to the Organization and Government.

While LAUNCH requires employees, Board members, and contractors to report Compliance Issues directly to LAUNCH, certain laws provide that individuals may also bring their concerns directly to the government. Any perceived retaliation or intimidation should be reported to the Compliance Officer immediately.

3. Confidentiality.

Anyone who investigates a Compliance Issue shall maintain the confidentiality of the individual who made the report if the individual has requested confidentiality or reported through a confidential reporting mechanism, unless the matter is subject to a disciplinary proceeding, referred to or under investigation by the New York State Attorney General's Medicaid Fraud Control Unit ("MFCU"), the New York State Office of the Medicaid Inspector General ("OMIG"), or law enforcement, the disclosure is required during a legal proceeding, or when otherwise required by law or contract.

4. Statutory Protections.

In addition to the protections afforded to employees, Board members, and contractors under this Policy, the following New York State laws also protect employees from retaliatory action for good faith reporting.

   a. New York State Labor Law, Section 740.

An employer may not take any retaliatory action against an employee if the employee discloses, or threatens to disclose, information about the employer's policies, practices, or activities to a regulatory, law enforcement, or other similar LAUNCH or public official.

Protected disclosures are those that assert that the employer is in violation of a law that creates a substantial and specific danger to the public health and safety, or which constitutes

health care fraud under Penal Law § 177[3] or Social Services Law § 145-b.[4] The employee's disclosure is protected only if the employee first raised the matter with a supervisor and gave the employer a reasonable opportunity to correct the alleged violation. Employees are also protected from retaliatory action if the employee objects to, or refuses to participate in, any activity that is in violation of a law that creates a substantial and specific danger to the public health and safety or which constitutes health care fraud under Penal Law § 177 or Social Services Law § 145-b.

If an employer takes retaliatory action against the employee, the employee may sue in State court for reinstatement to the same, or an equivalent position, any back wages and benefits, and attorneys' fees. If the employer is a health care provider and the court finds that the employer's retaliatory action was in bad faith, the court may impose a civil penalty of $10,000 on the employer.

b. New York State Labor Law, Section 741.

A health care employer may not take any retaliatory action against an employee if the employee discloses, or threatens to disclose, certain information about the employer's policies, practices, or activities to a regulatory, law enforcement, or other similar LAUNCH or public official, to a news media outlet, or to a social media forum available to the public at large.

Protected disclosures are those that the employee, in good faith, believes constitute improper quality of patient care or improper quality of workplace safety. The employee's disclosure is protected only if the employee first raised the matter with a supervisor and gave the employer a reasonable opportunity to correct the alleged violation, unless the danger is imminent to the public or a patient, and the employee has a good faith belief that reporting to a supervisor would not result in corrective action. Employees are also protected from retaliatory action if the employee objects to, or refuses to participate in, any activity, policy, or practice of the employer that the employee, in good faith, reasonably believes constitutes improper quality of patient care or improper quality of workplace safety.

If an employer takes retaliatory action against the employee, the employee may sue in State court for reinstatement to the same, or an equivalent position, any back wages and benefits, and attorneys' fees. If the employer is a health care provider and the court finds that the employer's retaliatory action was in bad faith, the court may impose a civil penalty of $10,000 on the employer.

[3] New York State Penal Law § 177 criminalizes knowingly filing, with intent to defraud, a claim for payment that intentionally has false information or omissions.

[4] New York State Social Services Law § 145-b criminalizes submission of false statements or deliberate concealment of material information in order to obtain public assistance, including Medicaid.

LAUNCH
Fueling Individualized Learning

Corporate Compliance

Policy on Policies
Policy 521

June 2023

Policy:

LAUNCH is committed to ensuring all state and federal regulations are adhered to and participants receive quality care. In order to accomplish this, standards are implemented to provide guidance for decision-making and to streamline internal processes.

Procedure:

- All policies will be drafted using the LAUNCH policy template.
- All new and revised policies will be shared with the appropriate people within 30 days. This should be documented in some way (staff meeting minutes, attestation, email read receipt, etc.)
- Each department has identified priority policies that are reviewed with all staff during orientation.
- Policies will reviewed as needed unless otherwise specified.

For Department Specific Standards:

- All policy drafts and revisions must be sent to the Associate Executive Director (AED) for review prior to implementation.
- The final policy will be saved to ADP for Human Resources related policies and shared gdrive folder for all other Policies in a PDF format.

For Agency Standards:

- All policy drafts and revisions are reviewed by the Associate Executive Director and the Executive Director.
- The draft will then be shared with the Management Team for discussion prior to being shared with the rest of the staff.
- The policy will be saved to ADP for Human Resources related policies and shared gdrive folder for all other policies in a PDF format.

For Compliance Policy Standards:

- All policy drafts and revisions are reviewed by the Associate Executive Director and the Executive Director.
- The draft will then be shared with the Board of Directors for final approval.
- The finalized standard will be saved to gdrive and on the website.
- Affected individuals will be informed of the updated/revised policy and instructed to share with their staff within 30 days.

- Compliance policies will be reviewed annually to ensure they are effective in meeting the goals of the compliance plan.

LAUNCH

Fueling Individualized Learning

Standards of Conduct

Policy 1010 Disciplinary Procedures, Board of Directors	June 2023

LAUNCH is committed to providing quality services and billing for services in a legal and ethical manner to ensure that the agency's reputation is protected, and the agency's mission is attained. LAUNCH has developed a Corporate Compliance plan in an effort to comply with applicable State and Federal laws. As a partner in conducting business, we expect all members of the Board of Directors will understand, support, and enforce LAUNCH's Compliance Plan and the policies contained therein in the original context and any revisions thereafter.

The purpose of an effective corporate compliance plan is to reduce waste and prevent fraud and abuse. Adhering to LAUNCH's corporate compliance plan is the responsibility of all affected individuals as defined by the Office of Medicaid Inspector General (OMIG) including, but not limited to all employees, the executive director, all senior administrators, managers, contractors, agents, subcontractors, independent contractors, the Board of Directors, and agency officers.

As a partner in service, the Members of the Board of Directors will review the Compliance Plan and all included policies during annual compliance training. Information can also be found at www.LAUNCHCNY.org and members may contact the Compliance Officer with any questions or concerns at Compliance@accesscny.org or 315-410–3318. The Compliance Plan will be updated as required and the most recent version will remain available at the above-provided link. If the laws, regulations, or policies change, the Board of Directors will review and approve all changes to agency policies.

In the event a Member of the Board of Directors violates the Compliance Plan the Board of Directors will determine the consequence which may include removal from the Board of Directors.

Please refer the Compliance Plan(Policy # 506) and associated policies including the Compliance Committee Charter(Policy 506A) and the Board By-Laws for further guidance.

LAUNCH

Fueling Individualized Learning

Standards of Conduct

Discipline Procedures Vendors and Contractors **June 2023**
Policy 1011

LAUNCH is committed to providing quality services and billing for services in a legal and ethical manner to ensure that the agency's reputation is protected, and the agency's mission is attained. LAUNCH has developed a Corporate Compliance plan in an effort to comply with applicable State and Federal laws. As a partner in conducting business, we expect all vendors and contractors and their staff will understand, support, and enforce LAUNCH's Compliance Plan and the policies contained therein in the original context and any revisions thereafter.

The purpose of an effective corporate compliance plan is to reduce waste and prevent fraud and abuse. Adhering to LAUNCH's corporate compliance plan is the responsibility of all affected individuals as defined by the Office of Medicaid Inspector General (OMIG) including, but not limited to all employees, the executive director, all senior administrators, managers, contractors, agents, subcontractors, independent contractors, the Board of Directors, and agency officers.

As a partner in service, we require Vendors and Contractors to annually review the Compliance Plan and all included policies at www.LAUNCHCNY.org and contact our Compliance Officer with any questions or concerns at Compliance@accesscny.org or 315-410–3318. The Compliance Plan will be updated as required and the most recent version will remain available at the above-provided link. If the laws, regulations, or policies change, your acceptance of the same is automatically deemed revised unless otherwise provided in writing.

In the event a vendor or contractor violates the Compliance Plan and the obligations set therein, LAUNCH may opt to terminate the relationship and cease conducting business with the vendor and/or contractor acting in a manner that violates the Compliance Plan.

Please refer the Compliance Plan(Policy #506) and associated policies.