Changing Lives...
Building Communities ™

CORPORATE COMPLIANCE PROGRAM

Catholic Charities Brooklyn and Queens
and Affiliates

Catholic Charities Neighborhood Services, Inc. (CCNS)
Catholic Charities Progress of Peoples Development Corporation (CCPOPD)
Progress of Peoples Management Corporation (POPM)

1/2011; rev. 2/2017; rev. 9/2017; rev. 12/2019; rev. 8/2021; rev. 11/2022; rev. 3/2023

INDEX

I. Introduction

II. Mission

III. Code of Ethics

IV. Best Practices

V. Policies

Clients and Their Records

Policy 0: Commitment to Compliance

Policy 1: Client's Privacy

Policy 2: Client Access to Services

Policy 3: Serving Minors Without Parental Consent

Policy 4: Client's Right to Refuse Treatment or Services

Policy 5: Contents of Client File/Record

Policy 5A: Red Flags Rule

Policy 6: Access, Release, Uses and Disclosures of Client Records/Information

Policy 7: Clients' Access to Their Own Records

Policy 8: Clients' Rights to Amend or Insert Comments In Their Records

Policy 9: Client Right to Accounting of Disclosure of Information

Policy 10: Behavior Management

Policy 11: Incident Abuse/Reporting

Policy 12: Duty to Warn – Disclosure of Information

Policy 13: Research Involving Agency Clients

Policy 14: Consent for Taking and for Use of Photographs/Videotape

Ethical Behavior in the Workplace

Policy 15:	Ethical Behavior
Policy 15A:	Compliance as Job Responsibility
Policy 15B:	Discipline
Policy 15C:	Use of Agency Resources and Funds
Policy 16:	Corporate Compliance Training and Education
Policy 17:	Employee Conflict of Interest
Policy 18:	Board Conflict of Interest
Policy 19:	Whistleblower/Reporting Non-Compliance
Policy 19A:	Non-Retaliation/Non-Intimidation
Policy 20:	Protection of Client Funds
Policy 21:	False Claims Act
Policy 22:	Auditing and Monitoring
Policy 22A:	Clients Rights
Policy 22B:	Client Grievance Policy

Security Policies

Policy 23:	General Computer Use
Policy 24:	User Password
Policy 24A:	Multi-Factor Authentication
Policy 25:	E-Mail/Other Electronic Communications Acceptable Use
Policy 26:	Internet Use
Policy 27:	**Temporarily Omitted**
Policy 28:	Use of Agency Computers/Devices for Agency Work
Policy 28A:	Receipt and Return of Agency Devices
Policy 29:	**Temporarily Omitted**
Policy 30:	Computer Information Systems Security Training
Policy 31:	Fax Policy

Policy 32: Record Retention

Policy 33: Controls for Physical Access to Agency Premises

Miscellaneous

Policy 34: Continuous Quality Improvement

Policy 35: Use of Agency Attorneys

Policy 36: Contracting Standards

Policy 37: Contractor Selection

Policy 38: Supervision

Policy 39: Breach Notification

Policy 40: Responding to Compliance Issues

Policy 41: Compliance Program Review

Policy 42: Measuring Effectiveness

INTRODUCTION

I. The Purpose of This Compliance Program

The Agency Corporate Compliance Program (the "Compliance Program") is designed to reflect the Agency's Mission, Ethical Standards, Best Practices and to promote the Agency's compliance with the Medicaid program and applicable federal, state and local laws and regulations as well as government contracts and conditions of participation in public programs. The primary goals of the Compliance Program are to:

- Prevent fraud, abuse and other improper activity in connection with the Medicaid program requirements as well as other laws, rules, regulations and Agency policies and procedures by creating a culture of compliance within the Agency;
- Detect any misconduct that may occur at an early stage before it creates a substantial risk of civil or criminal liability for the Agency; and
- Respond swiftly to compliance problems through appropriate disciplinary and corrective action.

The Compliance Program reflects the Agency's commitment to operating in accordance not only with the strict requirements of the law, but also in a manner that is consistent with high ethical and professional standards. The Compliance Program applies to the full range of the Agency's activities.

Applicability

Risk areas. The compliance program shall apply to the Agency's risk areas, which are those areas of operation affected by the Compliance Program and shall apply to:

(1) billings;

(2) payments;

(3) ordered services;

(4) medical necessity;

(5) quality of care;

(6) governance;

(7) mandatory reporting;

(8) credentialing;

(9) contractor, subcontractor, agent or independent contract oversight

(10) other risk areas that are identified by the Agency through its organizational experience.

Employees and Other Affected Individuals. The Compliance Program applies to all individuals who are affected by the Agency's risk areas. The following persons are subject to the Compliance Program:

- All affected employees
- The Chief Executive, senior administrators, managers
- Governing Body and corporate officers
- Any person or affiliate who is involved with the Agency such that the person or affiliate contributes to the Agency's entitlement to payment under the Medical Assistance Program (Medicaid Program) and who is not an employee, Executive, or Governing Body member of the Agency (e.g., contractors, subcontractors, agents, independent contractors, interns, students, volunteers, and vendors).

The above persons shall be referred to as **"employees and other affected individuals"** throughout the Compliance Program.

All employees and other affected individuals have a personal obligation to assist in making the Compliance Program successful. Employees and other affected individuals are expected to:

(1) familiarize themselves with the Compliance Program's Standards of Conduct and compliance procedures;
(2) review and understand the key policies governing their particular job/service functions;
(3) report any fraud, abuse or other improper activity through the mechanisms established under the Compliance Program;
(4) cooperate in Agency audits and investigations; and
(5) carry out their jobs/provision of services in a manner that demonstrates a commitment to honesty, integrity and compliance with the law.

The Compliance Program is regularly reassessed and is constantly evolving to address new compliance challenges and maximize the use of Agency resources.

II. The Elements of the Compliance Program

The key elements of the Compliance Program are as follows:

- Standards of Conduct;
- The assignment of personnel to oversee the Compliance Program, including the Compliance Officer and Compliance Committee;
- Compliance training for employees and other affected individuals;

- Mechanisms for reporting compliance problems, including an anonymous reporting option, and a prohibition on retaliation against employees and other affected individuals;
- Procedures for investigating reports of suspected compliance problems and cooperating in government investigations;
- A system of internal compliance audits and reviews to detect potential fraud, abuse or other improper activity;
- Procedures for taking corrective action in response to identified compliance problems ; and
- The imposition of disciplinary measures against employees and other affected individuals who engage in misconduct or fail to adhere to the terms of the Program.

III. Standards of Conduct

The Standards of Conduct set forth the basic principles that guide Agency decisions and actions. All employees and other affected individuals are expected to familiarize themselves with the Standards of Conduct and should rely on the standards contained in the Code in carrying out their duties.

The Standards of Conduct are not intended to address every potential compliance issue that may arise in the course of the Agency's business. The Agency has adopted detailed written policies governing its operations. Employees and other affected individuals are required to review and carry out their duties in accordance with the policies applicable to their job functions/provision of services. The Standards of Conduct's standards are set forth below.

1. Proper Billing for Services

The Agency obtains reimbursement from multiple government programs such as Medicaid, Medicare and state and local government agencies for the provision of health care and other services to its clients. Accurate billing is a key legal obligation which involves documenting and billing all services in accordance with all applicable laws, rules, conditions of participation and guidelines relating to the billing process. Employees and other affected individuals must ensure that Agency does not:

- Bill for clients not actually served by Agency;
- Bill twice for the same service;
- Bill at a rate in excess of the rate permitted under the applicable program;
- Bill for services the employees and other affected individuals knows are also being billed to the government through another source; or
- Bill the Medicaid program as the primary payor when the client has other public or private health insurance coverage.

All services rendered to clients must be appropriately documented according to Agency policies.

It is a violation of the *False Claims Act* to knowingly submit a false or fraudulent claim for payment to a federal program such as Medicaid or Medicare (See Compliance Policy 21, *False Claims Act*). Failure to comply with the *False Claims Act* may subject the Agency to criminal and civil penalties. Employees and other affected individuals involved in delegating billing to third party vendors must provide clear direction on proper billing procedures and monitor the vendors carefully.

2. Providing Access to Necessary Services

In accordance with Agency policies and procedures, all clients are treated equally and without favoritism. Accessibility to services shall be provided based upon need without regard to ability to pay, race, color, creed, national origin, gender or any other form of prohibited discrimination. All programs shall deliver services in accordance with eligibility criteria established by contract. If the requested services are not available at the program or within the Agency, appropriate referrals shall be made when possible. (See Compliance Policy 2, *Client Access to Services*)

3. Avoiding Kickbacks and Referral Fees

Under the federal Anti-Kickback Statute, it is illegal for any employees and other affected individuals to knowingly and willfully solicit, receive, offer or pay anything of value to another person in return for the referral of a client, or in return for the purchasing, leasing, ordering or arranging for any item or service reimbursed by a federal health care program such as Medicaid or Medicare. New York State has a similar Anti-Kickback law. There are serious penalties for violating these statutes.

4. Avoiding Conflicts of Interest

Employees and other affected individuals are required to act solely in the best interests of the Agency when carrying out their job responsibilities/provision of services and must avoid all activities that constitute or create the appearance of a conflict of interest. Employees and other affected individuals are prohibited from using their position with the Agency for personal benefit. For example, employees are prohibited from accepting gifts of more than nominal value from vendors of the Agency or facilitating contracts between the Agency and companies in which they have a financial interest.

The Agency has adopted an Employee Conflicts of Interest Policy that contains standards and procedures for avoiding conflicts of interest. All employees are expected to familiarize themselves with this policy. As a condition of employment, each employee must complete and sign an acknowledgment

stating that the employee fully understands his/her obligations under the policy and acknowledges his/her commitment to comply with the policy as an employee of the Agency. (See Compliance Policy 17, *Employee Conflicts of Interest*)

The Agency's Trustees, Directors and Officers are also required to avoid conflicts of interest. Among other things, they are prohibited from voting on or otherwise influencing the implementation of business arrangements between the Agency and the Trustee/Director/Officer or a company in which the Trustee/Director/Officer has a financial interest.

The Agency has adopted a Board Conflicts of Interest Policy. All Trustees, Directors and Officers are expected to familiarize themselves with this policy. Trustees, Directors and Officers are required to submit annual conflict of interest disclosure forms. (See Compliance Policy 18, *Board Conflicts of Interest*)

5. Using Agency Resources Exclusively for Agency Business

Employees and other affected individuals may use the Agency's resources solely for the purpose of carrying out their job responsibilities/provision of services. The Agency's facilities, equipment, staff and other assets may not be used by an employees and other affected individuals for personal benefit or to engage in any outside business or volunteer activity without the prior approval of the Compliance Officer. Employees and other affected individuals may not use their affiliation with the Agency to promote any business, charity or political cause. Employees shall seek reimbursement for expenses only to the extent such expenses have been incurred in the course of carrying out their job duties and in accordance with the Agency's expense reimbursement policies.

6. Using the Agency's Resources Exclusively for Charitable Purposes

The Agency is a tax-exempt organization under Section 501(c)(3) of the Internal Revenue Code which requires the Agency to engage in only those activities that are within its approved charitable purpose. Employees and other affected individuals may not use the Agency's resources to engage in any political or business activity that is outside the scope of the Agency's charitable purpose.

7. Ensuring Equal Opportunity for all Clients, Employees and Contractors

The Agency is committed to serving all clients on an equal basis without regard to race, nationality or ethnic origin, religion, gender, disability or any other personal characteristic with respect to which discrimination is barred by law. Discrimination on these grounds is also prohibited in connection with the hiring and treatment of employees and contractors. In addition, sexual harassment of employees or clients will not be tolerated. The Agency seeks to create an environment in which the dignity of each individual is fully respected.

8. Maintaining the Confidentiality of Client Records

All client records must be kept confidential in accordance with applicable privacy laws and regulations. The Agency is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which limits the use and disclosure of protected health information. The Agency also must comply with special state confidentiality laws governing client records and HIV-related information. The Agency has adopted a number of policies governing the use and disclosure of client records. All employees and other affected individuals who have access to such records must familiarize themselves with these policies and procedures, and adhere to their terms. (See Compliance Policy 6, *Access, Release, Uses and Disclosures of Client Records*)

9. Conducting all Business with Honesty and Integrity

The Agency is committed to conducting all of its activities with honesty and integrity. Employees and other affected individuals are expected to act in a manner that promotes the Agency's reputation as an organization that exceeds the strict requirements of the law and operates in accordance with the highest ethical standards (see Mission Statement, Best Practices and Code of Ethics).

IV. Compliance Oversight Personnel

1. Compliance Officer

The Compliance Officer is responsible for overseeing the implementation and modification of the Compliance Program. The Compliance Officer's chief duties include, but are not limited to, the following:

- Overseeing and monitoring the adoption, implementation and maintenance of the compliance program and evaluating its effectiveness;
- Drafting, implementing, and updating no less frequently than annually or, as otherwise necessary, to conform to changes to Federal and State laws, rules, regulations, policies and standards, a compliance work plan which outlines the Agency's proposed strategy for meeting the requirements for a compliance program for the coming year, with a specific emphasis on written policies and procedures, training and education, auditing and monitoring, and responding to compliance issues.
- Reviewing and revising the Compliance Program and the written policies and procedures and standards of conduct, to incorporate changes based on the Agency's organizational experience and promptly incorporate changes to Federal and State laws, rules, regulations, policies and standards;
- Reporting directly, on a regular basis, but no less frequently than quarterly, to the Agency's governing body, chief executive, and Compliance

Committee on the progress of adopting, implementing, and maintaining the Compliance Program;

- Assisting the Agency in establishing methods to improve the Agency's efficiency, quality of services, and reducing the Agency's vulnerability to fraud, waste and abuse;
- Investigating and independently acting on matters related to the Compliance Program, including designing and coordinating internal investigations and documenting, reporting, coordinating, and pursuing any resulting corrective action with all internal departments, contractors and the State
- Overseeing operation of the Compliance Hotline;
- Receiving, evaluating and investigating compliance-related complaints, concerns and problems;
- Ensuring proper reporting of violations to duly authorized enforcement agencies as appropriate or required;
- Working with the Office of Human Resources and others as appropriate to develop the compliance training program; and

The Compliance Officer reports to the Chief of Staff who reports to the Chief Executive Officer (the "CEO"). The Compliance Officer makes annual and as needed reports to the Audit Committee of the Board of Trustees on the operation of the Compliance Program as well as quarterly reports to the Catholic Charities Neighborhood Services, Inc. Board of Directors.

Employees and other affected individuals should view the Compliance Officer as a resource to answer questions and address concerns related to the Compliance Program or compliance issues.

2. Compliance Committee

The Compliance Committee shall be responsible for coordinating with the Compliance Officer to ensure that the Agency is conducting its business in an ethical and responsible manner, consistent with its Compliance Program. The Compliance Committee Charter outlines the duties and responsibilities, membership, designation of a chair and frequency of meetings. The Compliance Committee shall meet at least quarterly and shall review and update the Compliance Committee Charter annually. The Compliance Committee shall report directly and be accountable to the Agency's Chief Executive and governing body.

The Compliance Committee shall be comprised of senior managers and the Compliance Officer will seek to appoint employees with varying backgrounds and experience to ensure that the Compliance Committee has the expertise to handle the full range of clinical, administrative, operational and legal issues relevant to the Compliance Program. Compliance Committee shall be comprised of the Chief Compliance Officer, the Compliance Risk Officer, the Assistant Counsel, the

Deputy Chief Financial Officer, the Senior Vice Presidents/Chief Program Officers of CCNS, the Chief Privacy Officer, the Chief Security Officer, the Senior Vice President of the Office of Planning and Evaluation, the Senior Vice President of Human Resources and any other employees deemed necessary by the Chief Compliance Officer.

The Compliance Committee's functions include, but are not limited to, the following:

- Coordinating with the Compliance Officer to ensure that the written policies and procedures, and standards of conduct of the Compliance Program are current, accurate and complete and recommending and approving any changes to the Compliance Program;
- Approving the Compliance training program provided to employees and other affected individuals and ensuring that the training topics are timely completed;
- Approving the internal auditing plan carried out under the Compliance Program;
- Coordinating with the Compliance Officer to ensure communication and cooperation by affected individuals on compliance related issues, internal or external audits, or any other function or activity required by the Compliance Program;
- Reviewing and confirming the adequacy of all investigations of suspected fraud or abuse and any corrective action taken as a result of such investigations;
- Advocating for the allocation of sufficient funding, resources and staff for the Compliance Officer to fully perform their responsibilities;
- Ensuring 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; and
- Advocating for adoption and implementation of required modifications to the Compliance Program.

3. Board of Trustees

The Board of Trustees has ultimate authority for the governance of the Agency, including oversight of the Agency's compliance with applicable law. The Board of Trustees has delegated authority for overseeing activities of the Compliance Officer and Compliance Committee as well as the general operation of the Compliance Program to the Audit Committee of the Board.

The Audit Committee receives reports on the operation of the Compliance Program directly from the Compliance Officer annually and as needed. The Compliance Officer has the right to bring matters directly to the Audit Committee's attention at any time.

The Catholic Charities Neighborhood Services, Inc. Board of Directors, as the Board with governance authority over the Agency programs participating in the Medicaid Program, receives Compliance reports throughout the course of the year at its regularly scheduled Board meetings.

V. Compliance Training

The Agency shall develop and maintain a compliance training plan. The training plan shall, at a minimum, outline the subjects or topics for training and education, the timing and frequency of the training, which affected individuals are required to attend, how attendance will be tracked, and how the effectiveness of the training will be periodically evaluated. Affected individuals shall receive annual Compliance training.

Every employee must attend the basic compliance training session offered by the Agency within 30 days of the commencement of employment. This session covers the contents of the Standards of Conduct and the key elements of the Compliance Program. Employees must acknowledge in writing that they have received this training and understand the Standards of Conduct. Employees are required to participate in any advanced compliance training sessions organized by their department/program, which are designed to focus on the specific compliance issues associated with the department/program's functions.

Other affected individuals will receive Compliance training within 30 days of the commencement of their relationship with the Agency and periodic trainings thereafter. Compliance training will include compliance issues, compliance expectations, and compliance program operations.

VI. Reporting Compliance Problem

1. Reporting Options

In accordance with Compliance Policy 19, *Whistleblower/Reporting Non-Compliance*, which relates to the reporting of fraud, abuse or other violations, the Agency maintains open lines of communication for the reporting of suspected improper activity. Employees and other affected individuals are expected to promptly report any such activity of which they become aware in one of the following ways:

- Notify their supervisor, director, vice president, or senior vice president who will in turn, notify the Compliance Office;
- Notify the Compliance Office;
- File a report through the Compliance Hotline.

2. Compliance Hotline

The Compliance Hotline may be accessed by dialing 1(800)493-8330. To encourage full and frank reporting of suspected fraud or abuse, the Agency gives employees and other affected individuals the option of filing complaints anonymously through the Compliance Hotline. (Compliance Policy 19, *Whistleblower/Reporting Non-Compliance*) The Compliance Officer is responsible for reviewing all Compliance Hotline reports, assessing whether they warrant further investigation and ensuring that any compliance problems are identified and corrected.

Employees should understand that the Compliance Hotline is designed solely for the reporting of fraud, abuse and other compliance problems; it is not intended for complaints relating to the terms and conditions of an employee's employment with the Agency. Any such complaints should be directed to the Office of Human Resources.

3. Non-Retaliation

Employees and other affected individuals who participate in good faith in the Compliance Program by reporting suspected fraud, abuse or other improper activity; by cooperating in investigations, self-evaluations, audits and corrective actions; and by reporting to appropriate officials as provided in Sections 740 and 741 of the New York State Labor Law, will not be subject to retaliation by the Agency in any form. Prohibited retaliation includes, but is not limited to, terminating, suspending, demoting, failing to consider for promotion, harassing or reducing the compensation of any employee due to the employee's intended or actual filing of a report. Employees and other affected individuals should immediately report any such retaliation to the Compliance Office. (See Compliance Policy 19A, *Non-Retaliation/Non-Intimidation*)

VII. Investigations

1. Internal Investigations

All reports of fraudulent, abusive or other improper conduct, whether made through the Compliance Hotline or otherwise, are promptly reviewed and evaluated by the Compliance Office. The Compliance Office shall determine, whether the report warrants an internal investigation. If so, the Compliance Office coordinates the investigation, issues a written report of its findings and proposes any corrective action that may be appropriate as per the Compliance Office Guidelines.

2. Government Audits and Investigations

Employees and other affected individuals are expected to fully cooperate in all government audits and investigations. Any employee or other affected individuals who fails to provide such cooperation will be subject to termination of

employment, if an employee or termination of role with the Agency for other affected individuals. (See Compliance Policy 15A, *Corporate Compliance as Job Responsibility*)

All subpoenas and other governmental requests for Agency documents should be forwarded to the Office of Legal Affairs which is responsible for reviewing and responding to such requests. (See Compliance Policy 35, *Use of Agency Attorneys*). Employees and other affected individuals are strictly prohibited from destroying, improperly modifying or otherwise making inaccessible any documents that the employee or other affected individual knows or has reason to know are the subject of a pending government subpoena or document request. Employees or other affected individuals also are barred from directing or encouraging another person to take such action. These obligations override any document destruction policies that would otherwise be applicable. (See Compliance Policy 32, *Record Retention*)

If an employee or other affected individual receives a request from a government investigator to provide an interview, the employee or other affected individual should immediately contact his or her supervisor, for employees, or other Agency contact for other affected individuals. The supervisor/Agency contact will inform the Office of Legal Affairs. The Office of Legal Affairs will seek to coordinate and schedule all interview requests with the relevant government agency. Employees or other affected individuals are expected to answer all questions posed by government investigators truthfully and completely.

VIII. Compliance Audits and Reviews

The Agency seeks to identify compliance issues at an early stage. One of the methods of achieving this goal is the performance of regular internal audits and compliance reviews.

The Compliance Audits provide a method by which to review risk areas identified by the Corporate Compliance Program. The Compliance Office will request annual audits, random audits, as needed audits as a result of complaints and external audits, if necessary. The Compliance Officer will seek input on development of audit plans from the Audit Committee.

The Office of Planning and Evaluation will complement the Corporate Compliance Program by bringing to the attention of the Compliance Office any matters which demonstrate non-compliance with the Compliance Program. A member of the Office of Planning and Evaluation will be a member of the Compliance Committee.

The Compliance Office will develop a work plan for a schedule of internal audits. The audits cover aspects of the Agency's operations that pose a heightened risk of non-compliance, including but not limited to, Medicaid/Medicare billing and access to services. A written report is submitted to the Compliance Office by the audit team summarizing the findings of each audit and recommending any appropriate corrective action. (See Compliance Policy 22, *Compliance Audit*)

Employees and affected individuals are required to participate in and cooperate with internal audits and implementation of any corrective action plans.

IX. Corrective Action

The Agency is committed to taking prompt corrective action to address any fraud, abuse or other improper activity identified through internal audits, investigations, reports by employees, other affected individuals or by other means. The Compliance Office is authorized to recommend corrective action to the Chief Executive Officer or directly to the Board of Trustees. In cases involving clear fraud or illegality, the Compliance Office also has the authority to order interim measures, such as a suspension of billing, while a recommendation of corrective action is pending.

Corrective action may include, but not be limited to, any of the following steps:

- Modifying the Agency's existing policies, procedures or business practices;
- Providing additional training or other guidance to employees and other affected individuals;
- Seeking interpretive guidance of applicable laws and regulations from government agencies;
- Disciplining/terminating employees/other affected individuals;
- Notifying law enforcement authorities of criminal activity by Affected Individuals;
- Returning overpayments or other funds to which the Agency is not entitled to the appropriate government agency or program; or
- Self-disclosing fraud or other illegality through established state and federal self-disclosure protocols.

X. Employee Discipline/Other Affected Individuals Termination

Employees who engage in fraud, abuse or other misconduct are subject to disciplinary action in accordance with the Agency's Disciplinary Policies, for employees (See Compliance Policy 15B, *Discipline*). Other affected individuals who engage in fraud, abuse or other misconduct are subject to termination of their role with the Agency.

Changing Lives...
Building Communities ™

Mission Statement

Catholic Charities of the Diocese of Brooklyn and Queens translates the Gospel of Jesus Christ into action by affirming the dignity and value of every person, especially the most vulnerable members of our diverse society. Catholic Charities develops effective responses to human need and joins with all people of good will in advocating for a social order which promotes justice and embraces human development.

STATEMENT OF VALUES - CODE OF ETHICS
CATHOLIC CHARITIES, DIOCESE OF BROOKLYN

PREAMBLE

Principles of Catholic Social Teaching

Human Dignity

- Catholic Charities affirm that each person is made in the image of God and has inherent dignity. Each person must be respected from conception to natural death. Each person is endowed with rights and duties.

- Catholic Charities affirm that each person served and engaged with our work will be held in great esteem and with great respect.

Common Good

- Catholic Charities affirm that there is a universal destination of all created things, that all persons have the right to access all that they need in order to reach their fulfillment and that all persons have the concurrent obligation to work for the rights of others as well.

Subsidiarity

- Catholic Charities affirm that decisions should be made at the lowest possible level, should involve those who are capable of participation in decision-making and who will be impacted by those decisions, and should empower those who are most in need. Concurrently, we commit to creating and renewing structures and institutions that provide assistance and aid, as required, appropriate and necessary.

- Catholic Charities, as members of the civic society, affirm that we should actively participate in the public discourse at both the national and local community level, seeking justice for all, but especially for those who have no voice of their own. We affirm that we should both advocate and serve, advocating both for individuals and for just social structures.

Solidarity with the Poor

- Catholic Charities affirm that the most poor and vulnerable persons and families have a special claim to our services and programs.

- Catholic Charities affirm that our staff and boards should engage those served to have representative voice in decisions impacting policies and programs. Accordingly, we affirm the need to create structures and processes for obtaining appropriate input from stakeholders.

- Catholic Charities commit ourselves to continue to be a voice with poor and vulnerable individuals and families in the public discourse.

Fundamental Values

Truth

- Catholic Charities affirm that transparency and accountability will always be pursued in our communication and work.

- Catholic Charities affirm the truth of the intrinsic dignity and worth of the human person as a social being and will witness to our Catholic identity in fulfilling our roles in Church and in society.

Freedom

- Catholic Charities affirm that we will always assist our clients, staff and volunteers to live in socially responsible freedom, to exercise their authentic autonomy in light of objective truth and to actualize their inherent potential as being created in the image and likeness of God.

- Catholic Charities will respect and affirm the autonomy of each organization/entity with whom we are in relationship.

Justice

- Catholic Charities affirm that it is a matter of justice that all clients have the right to self-actualization and to reach their potential as beings created in the image and likeness of God.

- Catholic Charities affirm that we will work to achieve greater justice in our communities through our social policy advocacy efforts – locally, nationally and internationally.

- Catholic Charities affirm that all contracts and agreements and all relationships with stakeholders will be based on norms of justice.

- Catholic Charities affirm that we will work to expand and maintain diversity and excellence in our membership, board, leadership positions and staff.

- Catholic Charities affirm that we will continue to work to help eradicate racism and prejudice within our own organizations and in society at large.

Love

- Catholic Charities affirm that love – caritas – will be the chief identifying characteristic and element of our work and life.

INTRODUCTION

At Catholic Charities, our mission is to reach out to and provide assistance to those in need – the poor, sick, aged, isolated, disabled and alienated – and to promote unity among all persons seeking to develop caring communities. This mission is founded in Catholic social teaching which has a special concern for the poor and vulnerable. Its principles recognize the life and dignity of the human person and our fulfillment through relationships with others, the right to those things required for human dignity including food, shelter, health care, education, employment, and that personal responsibility must be joined with social obligation.

While we embrace the diversity of our staff and those we serve, we recognize that as we carry out Catholic Charities' mission through our daily work lives, we must all be guided by core values and principles. These ethical principles guide our behavior and establish the guidelines to which we are accountable.

GOVERNANCE

Catholic Charities, Diocese of Brooklyn, has an active governing body whose members have the pre-requisite skills and experience to carry out their responsibilities. The governing body:

- Hires, evaluates and replaces when necessary the Chief Executive Officer (CEO).

- Holds the CEO responsible for providing the governing body with timely and accurate information on the cost of our services and financial operations.

- Ensures that we are knowledgeable and comply with all laws and regulations, which control our programs, human resources and fiscal operations.

- Oversees our resources and directs that they be prudently used and managed.

- Directs that there are effective accounting systems, internal controls and that all financial statements and accounting records fairly and accurately reflect all business transactions.

- Requires we have a "Conflict of Interest" policy that regulates the behavior of the governing body as well as the staff.

CONFLICT OF INTEREST

Catholic Charities, Diocese of Brooklyn, holds our governing body, management and staff to the highest principles of ethical behavior. The agency Conflict of Interest Policy requires:

- We must avoid any situation or interest which might interfere with our judgment with respect to our responsibilities to the agency or those we serve.

- We may never engage in any business or financial activity which may conflict or give the appearance of conflicting with the mission or purpose of the agency or the interests of those we serve.

- We may not enter into an independent business venture or perform work or services for another organization or business if these activities create a "conflict of time" with our responsibilities to the agency or those we serve.

- We must disclose any potential "conflict" to the agency's management and when appropriate to the governing body and those we serve.

- We may never accept a gift or gratuity from an individual we serve or a vendor of such value that it could be perceived by others as having the potential to interfere with our judgment in the performance of our duties.

CONFIDENTIALITY AND DISCLOSURE

Catholic Charities, Diocese of Brooklyn respects the rights of those we serve to confidentiality and the rights of our funders and supporters to a full accounting of how our funds are used. To fulfill these obligations:

- We accept our responsibility to provide comprehensive and timely information to all stakeholders: funders, donors, recipients of service

and the public regarding the services we provide, how our resources are allocated, and the policies and practices of the institution as long as the right to confidentiality is protected.

- We treat all non-public information as confidential and proprietary.

- We recognize the importance of maintaining complete and accurate records of all the services we provide and allow clients access to their records in accordance with accepted standards within the industry and in conjunction with Federal, State and Local regulations.

PROVISION OF SERVICE

Catholic Charities, Diocese of Brooklyn embodies within our services five core values: **social justice, dignity and individual worth of person, importance of human relationships, integrity, and competence**:

- We promote ***social justice*** by:

  1. Being the voice of those who are unable to advocate for themselves;

  2. Acting as an agent of change, joining with others to change systems and forces that promote oppression and prevent a person from living up to his/her potential;

  3. Encouraging the public to participate and support us in political and social actions that protect access to resources and services; and

  4. Expanding choices and eliminating discrimination against any individual, group or class.

- We honor the ***dignity and worth of individual persons*** we serve by:

  1. Acknowledging, respecting and validating the uniqueness of all persons;

  2. Being culturally competent and sensitive to the needs of the socially diverse populations we serve;

  3. Respecting the rights of those we serve to self-determination and informed consent by presenting them with their options, fully apprising them in understandable language of the benefits and risks of the service, the expectations of all participants, their right to withdraw from the service at any time and the consequences, if any, of that decision; and

4. Assuring those we serve both verbally and in writing that they have the right to privacy and confidentiality and that their information and records will only be shared with those who need to know.

- We recognize the ***importance of human relationships*** by:

1. Engaging those we serve as "partners" in their care, together building on individual and collective strengths to achieve positive outcomes and to promote the well-being of all;

2. Serving the most vulnerable members of our community and those most in need, by not passing judgment but by building relationships;

3. Being ever mindful of professional boundaries in our relationships with our colleagues and those we serve by never engaging in inappropriate physical contact, sexual relationships, sexual harassment, use of derogatory language, personally giving or borrowing money, accepting individual gifts, tips, favors and/or monetary remuneration for our services; and

4. Exercising discretion at all times when sharing our personal information or circumstances.

- We serve with ***integrity*** and behave in a trustworthy manner by:

1. Following through on our commitments and doing all it is that we say we will do;

2. Acting honestly, responsibly and refraining from activities that are, or can be perceived to be a conflict of interest;

3. Holding ourselves fully, consistently, and publicly accountable for compliance with established standards in program and fiscal operations and accepting responsibility to report failures to meet these standards by ourselves and others;

4. Seeking objective certification that we meet standards of quality in performance;

5. Staff clearly distinguishing when they are acting as a representative of the agency and accurately presenting the official and authorized positions of the organization; and

6. Never discriminating against any individual or group with respect to race, ethnicity, national origin, sex, sexual orientation, age marital status, political belief, religion, and mental or physical disability.

- We serve within our area of ***competence*** by:

    1. Committing to the continuing development of skills and knowledge to enhance our ability to serve others and increase awareness of ethical principles and practice;

    2. Accurately representing our professional credentials and areas of expertise;

    3. Using supervision to enhance our skills and to better meet the needs of those we serve; and

    4. Alerting a colleague and the Agency's Administration when we are concerned that the colleague is incompetent, unethical or that their ability to perform their function is impaired.

BEST PRACTICE #1

People are more than their statistics – we listen to their stories – understand their experience

BEST PRACTICE #2

We engage consumers as partners in the planning and service delivery process

BEST PRACTICE #3

We learn in the strengths and capacities of those we serve and build from there

BEST PRACTICE #4

We instill hope through our confidence that consumers can succeed

BEST PRACTICE #5

We believe in families – there are times when we serve as a substitute family

BEST PRACTICE #6

We tenaciously advocate for social justice

BEST PRACTICE #7

We know what is available for those we serve

BEST PRACTICE #8

We have integrity – we don't promise more than we can do and we do all that we say we can

BEST PRACTICE #9

We honor the dignity and uniqueness of those we serve

POLICY

The Agency is committed to and obligated to comply with all applicable federal and state standards.

PROCEDURE

1. The Agency shall identify governing laws and regulations that are applicable to its risk areas including any Medicaid Program policies and procedures as specified in 18 NYCRR PART 521.

2. The Agency shall comply with the following:

   New York State Laws and Regulations

   Social Services Law (SOS) § 363-d and 18 NYCRR Sub-Part 521-1 governing New York State Medicaid compliance program requirements.

   Social Services Law § 145
   Social Services Law § 145-b
   Social Services Law § 145-c
   Social Services Law § 363-d
   Social Services Law § 366-b
   Labor Law § 740
   Labor Law § 741
   State Finance Law §§ 187-194
   Penal Law Article 175
   Penal Law Article 176
   Penal Law Article 177
   18 NYCRR Part 521

   Federal Statutes and Regulations

   42 USC § 1396a(a)(68)
   31 USC §§ 3729-3733
   31 USC Ch. 38

3. The Agency will ensure that it establishes and maintains a culture of compliance in the Agency by providing annual and ongoing training to affected individuals and through supervision with employees and through oversight of relationships with other affected individuals.

CLIENTS' PRIVACY **POLICY NO. 1**

POLICY

The Agency strives for clients who live in Agency residences/apartments to live safely and with as much comfort, independence and dignity as possible. The Agency fully respects individual privacy and shall ensure privacy to the best of its ability. An exception is made when it is unsafe for a client due to his/her being a danger to himself/herself or others. The Agency provides clients with a statement of rights which fully outline his/her privacy rights. (See Policy 22A, *Clients' Rights*)

PROCEDURES

1. The client is given and shown a statement of client rights and responsibilities for the particular program. The client, parent or guardian is requested to review and sign the client rights and responsibilities so everyone is informed of the contents therein.

2. The Agency recognizes that clients' safety is paramount and recommends the following: (provided that it is in the best interest of the client and that privacy does not pose a danger to himself/herself or others).

   a. Maintain doors in sleeping areas and bathroom enclosures unless there is clear, clinical, justification for their removal;

   b. Provide assignment of one or two person rooms to persons who need extra sleep, protection from sleep disturbance, or who need privacy for clinical reasons;

   c. Require personnel to knock before entering a client's room;

   d. Require that established procedures for any legal searches of person or property be followed and documented:

   e. Require that procedures are followed which prohibit the search of persons residing in open facilities;

   f. Prohibit the use of surveillance cameras or listening devices for routine observation of clients in their rooms or other living areas;

   g. Provide adequate and safe storage for valuables and personal belongings.

POLICY

All clients are treated equally and without favoritism. Accessibility to services shall be provided based upon need without regard to ability to pay, race, color, creed, national origin, gender or any other form of prohibited discrimination. All programs shall deliver services in accordance with eligibility criteria established by contract. If the requested services are not available at the program or within the Agency, appropriate referral shall be made when possible.

PROCEDURES

1. The Vice President of the service area shall be responsible for ensuring each program is aware of and complies with all applicable laws, regulations and contract requirements for delivery of service within the program. The Vice President shall ensure that all program intake criteria and admissions/discharge criteria are non-discriminatory and are in accordance with this policy.

2. Programs shall conduct an initial screening to determine whether or not services are needed and whether the services can be provided at the program.

   a. If services cannot be provided at the program or within the Agency, the client shall be referred, if possible, to another provider.

   b. If there is a waiting list for the services, the program will determine whether or not the client requires services immediately. Based on the determination, the client will be placed on the waiting list or arrangements will be made for immediate services.

   c. Emergency situations are given priority. Any emergency services necessary to screen, stabilize and treat clients are not subject to pre-authorization or other utilization review procedures.

POLICY

A minor is a person under the age of 18 unless the person under age 18 is a parent of a child, a married person or an emancipated minor.

Parental/guardian consent shall be obtained before services are provided to minor children except under the following circumstances:

1. The minor is knowingly and voluntarily seeking the services
   and
2. The provision of services is necessary to the minor's well being
   and
3. A parent/guardian is not available
   or
   Requiring parental consent would have a detrimental effect on the course of treatment
   or
   The minor refuses to contact the parent/guardian.

In emergency situations requiring medical, dental, or hospital services, the program shall refer the minor for the appropriate emergency services and shall notify the parent/guardian as soon as possible.

PROCEDURES

1. When a minor seeks services and is not accompanied by a parent/guardian, the program shall speak with the minor about obtaining parental consent. If the minor does not wish to or cannot involve the parent/guardian, the program shall conduct the assessment listed above under policy.

2. The program manager shall determine whether services shall be provided to the minor and whether it is possible to resolve the parent/guardian conflict. The program manager shall contact the Vice President of the service area or the Office of Legal Affairs as needed.

3. All assessments and determinations shall be fully documented including a statement signed by the minor indicating that he/she is voluntarily seeking services.

4. The program shall advise the minor that the program shall contact the parent/guardian if an emergency situation arises or it is felt to be in the minor's best interest to contact the parent/guardian.

CLIENT'S RIGHT TO REFUSE TREATMENT OR SERVICES — POLICY NO. 4

POLICY

Clients have the right to refuse treatment, services and medication unless the right to refusal has been limited by law or court order.

Prior to commencement of services, clients should be informed of the plan for care, treatment, including any medications, and their right to refuse same.

PROCEDURES

1. The client/parent/guardian shall be informed of this policy at the time he/she first seeks services.

2. If a client/parent/guardian refuses or limits a plan of care and treatment including medication, a written note must be placed in the client's record. A refusal to take prescribed or recommended medication shall be related immediately to the physician, psychiatrist or other medically appropriate personnel.

3. All refusals or limitations of clinically and/or medically determined plans of care and treatment shall be reviewed with a supervisor to determine if an alternative plan of care or treatment is appropriate. If an alternative plan is deemed appropriate, the new plan shall be shared with the client/parent/guardian for his or her consent.

4. The treating employee shall discuss with his/her supervisor whether the refusal or limitation of a plan of care of treatment for a client contradicts or radically alters the nature of the service to be provided by the program or the eligibility criteria for receipt of services as established by the program.

5. If the client's refusal or limitation of the proposed plan of care and treatment is contrary to law, regulation, contract or program eligibility, the program may deny services or discharge the client from the program.

6. All decisions to modify or suspend services due to client/guardian/parent refusal shall be reviewed by the Vice President and any appropriate Agency committee to review such decisions.

CONTENTS OF CLIENT FILE/RECORD **POLICY NO. 5**

POLICY

The Agency shall maintain a separate and complete record/file, with up to date information, for all Agency clients.

The client file shall indicate the status of the case, i.e., whether it is open or closed. All files shall be maintained in a safe and secure environment subject to Agency policies on security and confidentiality of client information.

Agency programs shall adhere to all governing laws, rules and regulations applicable to the contents of client records and information.

PROCEDURES

1. All programs shall develop and update their client files from the time of intake/admission until discharge or closure.

2. The client file/record shall contain everything pertaining to the client and everything used to make decisions about the client including all relevant medical, psychological, social, financial, legal and demographic data as needed including, but not limited to, the following:

   a. name, date of intake/admission, date of birth, address and social security number;

   b. name and address of parents, legal guardians, qualified person and next of kin;

   c. emergency contact and/or qualified person's name, phone number and address;

   d. reason for admission, intake or referral;

   e. source of support and/or payment for services if relevant;

   f. medical history, if relevant to service to be provided and;

   g. source of referral, if applicable, and reports of previous evaluations;

   h. information regarding medication, prescription and monitoring;

   i. counseling sessions, start and stop times;

j. the modalities and frequencies of treatment furnished;

k. results of clinical tests, diagnosis, functional status;

l. the treatment/service plans, symptoms and prognosis;

m. progress notes and psychotherapy notes (if any);

n. in addition, for residential programs, detailed medical history, inventory of client possessions and plans for money management as needed.

Student's process/recording notes are not part of the client's record.

3. The client file shall be updated continuously with case notes and treatment data as services are provided. The client file shall contain progress notes, goals of service provision, both short and long term, and evaluation materials. Employees providing services to a client shall include their name on progress and treatment records added to the file. Supervisory review and comment on client treatment and service provision shall be so noted in the record. The form for the case notes, progress reports and treatment records shall be consistent with the requirements of the field of service and applicable contract requirements, laws and regulations.

4. When a client case is closed, the treating employee shall note the date of termination of services and prepare a termination summary. The record shall be stored in a manner consistent with the policy on closed files (See Compliance Policy 32, *Record Retention*).

POLICY

The Agency is committed to ensuring that it is in compliance with all federal, state and local laws, rules and regulations regarding identity theft including the Federal Trade Commission's *Identity Theft Prevention Red Flags Rule*. The Agency's Red Flags Rule Policy outlines how the Agency will identify, detect and respond to warning signs or "Red Flags" in its day to day operations.

This policy applies to Agency programs where the Agency is extending credit by accepting deferred payments for the purchase of services and where there is a reasonably foreseeable risk to clients or to the safety and soundness of the Agency from identity theft ("covered accounts").

The Compliance Office is responsible for oversight and administration of the policy. The Red Flags Rule Policy shall be reviewed and updated on an ongoing basis and as required by changes in laws, rules, regulations or Agency practices.

Identification of Red Flags

Red Flags generally fall into one of the following categories:

1. Suspicious documents;
2. Suspicious personal identifying information;
3. Alerts from others (e.g. client, identity theft victim or law enforcement)

Examples of Red Flags (the list is not exhaustive):

1. Documents provided for identification appear altered or forged.
2. Photograph on ID is inconsistent with appearance of client.
3. Information on ID is inconsistent with information provided by client.
4. Signature on ID is inconsistent with signature on other documents.
5. Suspicious address is supplied such as a mail drop or prison or phone numbers associated with pagers or answering services.
6. An address or telephone number is discovered to be incorrect, non-existent or fictitious.
7. Social Security number provided matches one submitted by another person.
8. An address or phone number matches that supplied by a large number of clients.
9. The client is unable to supply identifying information in response to notification that the application is incomplete.
10. Personal information is inconsistent with that already on file.
11. Client has an insurance number but never produces an insurance card or other documentation of insurance.
12. Complaint from client that he/she did not receive services for which he/she was billed.

13. Complaint from client that he/she is the victim of identity theft.
14. Notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency.

PROCEDURES

1. Detection of Red Flags

a. For new clients, the following identifying information/documentation will be required at the first appointment:

   i. Full name, date of birth, address on intake or application form
   ii. Driver's license or other photo ID
   iii. Current health insurance card
   iv. Utility bill or other correspondence showing residence if the photo ID does not show the client's current address

b. For minor clients, the parent/guardian will produce the information/ documentation listed above.

c. For existing clients, if the client has not visited the program for six months or more, employees will verify the information on file and update as necessary.

2. Response to Red Flags

a. An employee who becomes aware of any Red Flags involving inconsistent or suspicious information or documentation shall stop the intake/ admissions/six month verification process, immediately notify his/her supervisor and request that the client provide additional satisfactory information to verify identity.

b. If the client is unable or unwilling to produce additional satisfactory information/documentation, the intake/admissions/six month verification process shall terminate until such time as the client produces additional satisfactory information/documentation. The supervisor shall notify program management and the division administration as appropriate. The service area administration shall notify the Corporate Compliance Office which shall determine whether an investigation should be conducted and/or law enforcement notified.

c. If a client notifies an employee that the client did not receive services for which he/she was billed, the employee shall immediately notify the supervisor who shall notify program management and service area administration as necessary. The service area administration shall notify the Corporate Compliance Office which shall determine whether an investigation should be conducted and/or law enforcement notified.

d. If a client notifies an employee that the client believes he/she is a victim of identity theft, the employee shall immediately notify the supervisor who shall notify program management and service area administration as necessary. The service area administration shall notify the Corporate Compliance Office which shall determine whether an investigation should be conducted and/or law enforcement notified.

3. Training

a. All employees involved in client intake/admissions for programs with covered accounts as well as such employees' supervisors and program managers shall be trained in the Red Flags Rule Policy within thirty (30) days of the implementation of this policy. New employees will be trained in the Red Flags Rule Policy within thirty (30) days of the date of hire. In the event there are changes to the Red Flags Rule Policy, the above employees will be re-trained within sixty (60) days of the implementation of the change(s).

b. Employees will sign an acknowledgment of training which will be maintained in the employee's personnel file.

ACCESS, RELEASE, USES AND DISCLOSURES OF CLIENT RECORDS/ INFORMATION
POLICY NO. 6

POLICY

The Agency is committed to preserving the privacy and confidentiality of all client records and protected health information (PHI). Client records and PHI shall be used and disclosed only as permitted under the Agency's policies and applicable laws.

All Agency employees and other affected individuals shall comply with the rules and regulations pertaining to confidentiality and disclosure of PHI as stipulated in the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) as well as other laws, rules and regulations.

This policy applies to current and former clients, living or deceased, minors, guardians and qualified persons.

Definition of Protected Health Information: Information about the physical or mental health condition of a client, the provision of health care or the payment thereof and which either identifies the client or could be used to identify the client.

PROCEDURES

1. Obtaining Client Consent

a. Employees shall inform clients, at the time of the first visit, of the *Privacy Notice of Information Practices* ("the Notice"). The employee shall review the Notice with the client, ensure that the client understands it and signs it. The signed Notice shall be filed in the client's record.

b. If a client chooses not to sign the notice, the reason shall be stated on the notice and placed in the client's record.

c. In addition, each client is required to sign a consent for the use and disclosure of PHI for the purposes of treatment, payment and health care operations which shall be filed in the client's record.

d. If a client chooses not to sign the notice, the reason shall be stated on the notice and placed in the client's record. Also, the employee should consult with the supervisor as to whether the Agency should accept the client.

2. Authorization for the Procurement and Disclosure of Client Record/Protected Health Information

a. Except as described in 2C below, the employee shall not use or disclose a client's record/PHI without the client's authorization. An employee must obtain an authorization for procurement and disclosure to use PHI for specified purposes which are other than for treatment, payment or health care operations and to disclose PHI to third parties specified by the client.

b. If the employee who provides primary treatment or service responsibilities determines that an authorization for procurement or disclosure of PHI is required, the employee will have the client complete the authorization and will file it in the client's record.

c. An authorization is not required for the following uses and disclosures of client records/PHI (the list is not exhaustive):

- As emergency situations are occurring
- To the individual consumer
- To provide treatment
- To obtain and or receive payment for services
- To carry out health care operations
- To public health authorities who are legally authorized to receive such reports
- For the purpose of preventing or controlling disease, injury or disability, such as reports of known or suspected child abuse or neglect
- To insure continuous quality improvement of agency operations
- When required to do so by law enforcement or court orders
- If a correctional facility requires it by law
- To comply with Worker's Compensation law or for purposes of obtaining payment for any health care provided to the injured or ill worker.
- To a Business Associate for purposes of carrying out the Agency's treatment, payment or health care operations as long as the Agency has obtained satisfactory assurance via a written agreement that the business associate will appropriately safeguard the information

- To list client's name in a Directory that may be provided to members of the clergy.

- To notify and communicate with client's family or personal representative about his or her location, general condition or death.

- To coroners, medical examiners and funeral directors on the occasion of the client's death

- For specialized government functions such as national security

d. When authorization for procurement or disclosure of PHI is given, an employee will use the minimum necessary standard. This standard requires an employee to only supply what is asked for to satisfy the request. The minimum necessary standard does not apply when disclosing information for treatment purposes or to disclosures made pursuant to the individual's authorization.

3. Consent and Authorization by Persons Other than Client

a. For a client who is incapable of exercising his/her right to consent, a guardian or other legally authorized person may exercise consent or control the use and disclosure of the client's record/PHI.

b. A person is legally authorized to act on behalf of a client if he/she has been given authority by either the client's estate or other applicable law to act on behalf of the individual in making health care related decisions. It is usually the personal representative or guardian or in the case of a deceased person, the executor or personal representative. Documentation of legal representatives of client shall be contained in the client's record.

c. Under certain circumstances, the Agency will not recognize the authority of a personal representative to act on behalf of the client. These circumstances are when the Agency has a reasonable belief that:

i) The client has been or may be subject to domestic violence, abuse or neglect by such person; or
ii) Treating such person as the personal representative could endanger the client; and
iii) In the exercise of professional judgment, the Agency decides that it is not in the best interest of the client to treat the person as the client's personal representative.

d. Deceased Clients

The following persons may control the use or disclosure of a deceased client's record/PHI:

i) The next of kin (i.e., mother, father, husband, wife etc.)

ii) Personal representatives such as:

- Authorized by the deceased
- Power of attorney
- Executor under a will
- Personal representative if no will
- The only surviving relative

e. Parents and Un-emancipated Minors

A parent is usually but not always the personal representative of the minor and can exercise the minor's rights with respect to PHI. There are several exceptions when a parent cannot control the use and disclosure of a child's PHI:

i) When a State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service and the minor consents to the health care.

ii) When a court determines or the law authorizes someone other than the parent to make treatment decisions, procurement or disclosure decisions about PHI for the minor.

iii) When a parent agrees to a confidential relationship between the minor and the physician.

iv) Under the circumstances listed in 3 C above.

CLIENTS' ACCESS TO THEIR OWN RECORDS — POLICY NO. 7

POLICY

Clients may, under appropriate circumstances, have access to their own records and also, may make amendments to their records.

If the Agency believes that a client's access, to his/her records may be harmful to himself/herself or others, access may be denied.

Client records are property of the Agency; originals are never to be released to clients, parents or guardians.

PROCEDURES

Access in General

1. Should a client/parent/legal guardian wish to review a client's record, the request shall be made in writing to the appropriate employee at the program.

2. The employee receiving a request to review records shall immediately notify his/her supervisor.

3. Upon consultation with the treating practitioner(s), the program manager shall review the record, make a determination whether to permit access and if permitting access, shall do so within 10 days of the request.

4. If access is granted, the program shall determine whether it will review the record with the client on site or provide a copy of the record to the client.

5. A clinical record shall be defined as those materials relating to examination or treatment of the client prepared by the Agency. Materials prepared by other sources and provided to the Agency, shall not be released to clients/parents/guardians. Employees shall consider whether sensitive information about third persons contained in the record should be kept confidential.

Access to Minor's Records

6. If the client requesting records is a minor, the program shall follow the procedures above and in determining whether access is to be granted, shall take into consideration the age and maturity level of the minor.

   a. If the program determines access will be granted, the program will inform the minor that their parent/guardian will be notified of the granted request for review.

b. Should the minor object to parental/guardian notification, the program shall document the refusal and, provided that there is good cause, refrain from notifying the parent/guardian. The program reserves the right to notify the parent/guardian, regardless of the minor's objection, and the program shall inform the minor of this reservation.

c. If a parent/guardian of a minor requests access to the minor's record, the minor shall be informed of said request. Should the minor object to access to his/her records by his/her parent/guardian and the practitioner believes that access will have a detrimental affect on the practitioner/client or client/parent/guardian relationship, access will be denied to the parent/guardian in writing with the reason for denial stated therein.

Denial of Access

7. If access is denied the reasons for denial shall be provided to the client in writing. A request for records may be denied if there is reason to believe that review of the record will be harmful and have a detrimental effect on the client or others or on the practitioner/client relationship or client/parent/guardian relationship.

8. If access is denied, the program may elect to provide a prepared summary of the record to the client. Denial and/or access to client or minor client records shall be documented in the client's file. In addition, for minors, parental notification or minor's objection to parental notification also shall be documented in the record.

9. If a client is receiving services in a program operated or licensed by the Office of Mental Health or the Office for People with Developmental Disabilities, and access to his/her records is denied, the client shall be informed in the letter of denial that he/she may appeal the denial with the Clinical Records Access Review Committee convened by the Commissioner of the respective state agency.

10. Nothing in this policy or procedure shall be construed to limit a client/parent/guardians' right to access to records as set out in New York State Mental Hygiene Law Section 33.16 or Jonathan's Law.

CLIENTS' RIGHTS TO AMEND OR INSERT COMMENTS IN THEIR RECORDS

POLICY NO. 8

POLICY

Clients may make an amendment, correction or comment to their records.

PROCEDURES

1. A client who believes an entry in his/her record is incorrect or wishes to comment upon or amend the record, will be given a Health Record Correction/Amendment Form. An employee shall assist the client with the amendment/correction if necessary.

2. The completed Correction/Amendment Form will be sent to the original entry author for review and comment.

3. The entry author's review and comment shall be sent to the client.

4. All Correction/Amendment Forms and comments shall be signed.

5. If the correction/amendment is agreed upon by the client and entry author, the Form shall be placed in the record and forwarded to any parties who have previously received the record or others who may rely or have relied upon that information.

6. If the correction/amendment is not agreed upon by the client and entry author, both the corrections/amendments shall be placed in the record.

7. All disclosures of the Correction/Amendment Form shall be noted in the client's file. The notation shall indicate the date, by whom and to whom the record was sent.

8. A client's written comment(s) in relation to his/her treatment/service shall be placed in the client's record.

CLIENT RIGHT TO ACCOUNTING OF DISCLOSURE OF INFORMATION

POLICY NO. 9

POLICY

A client has a right to receive an accounting of disclosures of protected health information (PHI) during a time period up to six (6) years prior to the date of the written request for an accounting, except for disclosures:

- To carry out treatment, payment or health care operations as permitted pursuant to the client's consent;
- To the client about his or her own information;
- For the facility directory or to persons involved in the client's care;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials as permitted under law.

(See Compliance Policy 6, *Access, Release, Uses and Disclosures of Client Records/Information*)

PROCEDURES

1. A client's request for an accounting must be made in writing. The Agency must respond within thirty (30) days of receipt of the request. If unable to provide the accounting within thirty days, the time for response may be extended provided the client is given a written statement of the reasons for the delay and the date by which the accounting will be provided.

2. The accounting for each disclosure must include:

    - Date of disclosure;
    - Name of entity or person who received the PHI, and, if known, the address of such entity or person;
    - A brief description of the PHI disclosed;
    - A brief statement of the purpose of the disclosure.

If, during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, or pursuant to a single authorization, the accounting may provide the information as set forth above for the first disclosure, and then summarize the number disclosures made during the accounting period and the date of the last disclosure.

3. A separate log detailing the history of disclosures shall be maintained in the client's file.

4. The client's right to receive an accounting of disclosures of PHI made to a health oversight agency or law enforcement official can be suspended up to thirty (30) days upon the request of the agency or official.

5. The client should refer to the Agency's *Notice of Information Practices* for clarification of his/her rights regarding protected health information.

ACCOUNTING FOR DISCLOSURES LOG

Client Name: **Client Number:**

Date	Name of Entity or Person who received the PHI and Address (if known)	Brief Description of the PHI Disclosed	Purpose of the Disclosure	Check & Attach if Separate Author.

BEHAVIOR MANAGEMENT **POLICY NO. 10**

POLICY

The Agency provides services to its clients on a voluntary basis with the consent of the client, parent, or guardian. It is the Agency's policy to use the least restrictive means of intervention when a situation arises where a client is a danger to him/herself or others. Agency personnel are never permitted to use isolation, locked seclusion or mechanical restraints of any type when managing the behavior of a client of the Agency. Client records must be reviewed to ensure correct treatment is administered and authorized.

In all situations regarding the need for behavioral management, attempts at re-direction and verbal calming shall be used. The Agency prohibits use of restrictive techniques.

In addition, the Agency prohibits the following:

a. Degrading punishment;
b. Corporal or other physical punishment;
c. Forced physical exercise solely for the purpose of eliminating behavior rather than for instructive or athletic values;
d. Punitive work assignments;
e. Group punishment for behavior of one person served;
f. Medication for punishment;
g. Painful adverse stimuli used in behavior modification;
h. Interventions that involve withholding nutrition or hydration;
i. Interventions that inflict physical or psychological pain;
j. The use of demeaning, shaming, or degrading language or activities;
k. Punishment by peers;
l. Unwarranted use of invasive procedures and activities as a disciplinary action.

PROCEDURES

1. All Agency program staff shall use Verbal De-escalation techniques when a situation arises that calls for behavioral management. Training in Verbal De-escalation techniques shall be provided for all program management staff who will then be responsible for training their staff in these techniques.

2. In addition to Verbal De-escalation techniques, the following techniques will be used in the programs noted:

a. In the Agency's Early Childhood Programs, Day Care and Head Start educational staff and social service staff shall use the Montessori Method of Discipline and Positive Guidance Techniques. This method creates an environment that encourages positive behavior. The method includes specific techniques to redirect behavior and resolve disputes and set limits on physical contact for behavior modification. All interventions must be recorded in the child's file and shared with the parents/guardian.

b. In Agency programs serving clients with Alzheimer's or related dementia in congregate settings, employees must use only non-restrictive techniques to modify negative behaviors that are commonly expressed as the disease progresses. These techniques include having staff walk with a client to burn off excess energy or engaging a client in one-on-one activities instead of congregate activities in order to reduce the level of outside stimuli.

3. In rare situations where, despite all attempts at re-direction and verbal de-escalation, a client is still deemed to be a serious danger to him/herself or others, 911 may be contacted for Emergency Medical Service intervention.

4. A log of any intervention should be kept by each program for tracking purposes and trend analysis.

5. All clients, parents or guardians shall be advised of the Agency's Behavior Management Policy at the time of intake.

INCIDENT/ABUSE REPORTING **POLICY NO. 11**

POLICY

The Agency is committed to the protection of its clients, particularly the vulnerable, from abuse and neglect. Agency employees shall comply with all applicable laws, rules and regulations relating to the reporting of abuse, neglect or other incidents.

PROCEDURES

1. Agency employees shall be trained in and familiar with their duties and responsibilities for incident reporting under the laws, rules and regulations as required by New York State Offices of Mental Health and for People with Developmental Disabilities. The Agency has established an Incident Review Committee for Behavioral Health and an Incident Review Committee for Developmentally Disabled Persons which meet on a regular basis to review all incidents. The rules and regulations governing each committee shall be maintained by the Chair of each committee and the Agency's Director of Office of Planning and Evaluation and shall be shared with appropriate programs. Follow up to all incidents shall occur as required by regulations and shall be reviewed by the appropriate Project Director and Incident Review Committee.

2. Agency employees shall be trained in and be familiar with their duties and responsibilities under the law governing the reporting of suspected child abuse and neglect by mandated reporters.

3. Where programs do not have specific laws, rules and regulations for incident reporting, employees of such programs shall report all allegations of abuse, neglect or other serious incidents to the immediate supervisor. The immediate supervisor shall report the allegation to the Program Manager who will consult with the Vice President/Department Director regarding follow up to the incident.

DUTY TO WARN – DISCLOSURE OF INFORMATION POLICY NO. 12

POLICY

When a client is considered dangerous to himself/herself or others, the Agency shall take appropriate steps to provide the greatest possible protection to the client and the community.

PROCEDURES

1. While confidentiality of client information is of paramount importance, when a client poses a danger to himself/herself or others, confidential information may be shared with third parties but only such information which is necessary to protect the client and community.

2. Prior to disclosure of confidential information, an employee shall consult with the immediate supervisor and Program Manager. If necessary, the Program Manager shall consult with the Office of Legal Affairs.

3. Should an emergency situation preclude advance consultation, the employee shall take the necessary action to protect the client and community. As soon as possible thereafter the employee, shall report the incident and any disclosures made to the immediate supervisor and/or Program Manager.

4. Parents, legal guardians and next of kin shall be contacted regarding situations where a client may be harmful to himself/herself or others to the extent permissible by laws and regulations regarding confidentiality.

5. All emergency measures and disclosures shall be fully documented in the client's case record.

RESEARCH INVOLVING AGENCY CLIENTS **POLICY NO. 13**

POLICY

1. From time to time, the Agency may engage in research involving human subjects. The Agency has established policies and procedures to ensure that all research projects meet the highest standards to protect the human rights, confidentiality and privacy of Agency clients and staff.

2. All research projects involving Agency clients must be reviewed and approved by the Agency's Human Subjects Committee.

3. The Human Subjects Committee shall review research proposals that involve Agency clients; make recommendations regarding the ethics of proposed or existing research; make recommendations as to whether or not to approve research proposals and monitor ongoing research activities. The Human Subjects Committee shall be comprised of the Senior Vice President/Chief Program Officer and Vice President of the program under consideration for the research project; the Director of the Office of Planning and Evaluation; and a representative from the Office of Legal Affairs. The Senior Vice President/Chief Program Officer shall chair the committee. The Human Subjects Committee shall report to the Agency's Chief Executive Officer

4. Participation by a client as a subject in a research project is voluntary and shall not deprive any participant of any rights, privileges and protections provided to all other clients in Agency programs or facilities. Included in these rights is the right to give informed consent or withhold such consent for proposed research. A client may decline to participate in a research project without being denied Agency services.

5. Protecting the privacy of clients and the confidentiality of clients' information is of paramount importance to the Agency. The Human Subjects Committee shall ensure that any proposed research project has established appropriate procedures to ensure clients' privacy and confidentiality.

6. Informed consent must be obtained prior to a client's participation in any research project. The consent form shall include a statement that participation in the research project is voluntary, a statement that the Agency will continue to provide services to the client whether or not the client participates in the research project, an explanation of the nature and purpose of the research, a description of possible risks, a guarantee of confidentiality and the signature of the client, parent or guardian. A client may only take part in research which does not come into substantive conflict with his/her individual plan of services.

7. The Human Subjects Committee may elect to accept a University IRB review and approval in lieu of a full review provided that a copy of the approval and related study materials are on file.

PROCEDURES

1. All requests for research projects utilizing clients as subjects shall be submitted to the Chair of the Human Subjects Committee.

2. The Human Subjects Committee Chair shall distribute all relevant research project materials to the members of the Human Subjects Committee. The committee members shall review and consider: the purpose of the research project, potential benefits to the client and Agency, potential risks and concerns to/for the client and Agency, the procedures for privacy and confidentiality and the obtaining of informed consent, and any ethical issues presented by the proposed research.

3. The Human Subjects Committee shall make a determination as to whether or not the research project may be conducted and shall establish, when appropriate, a schedule for ongoing reporting to the Committee should the research project proceed. The Human Subjects Committee shall notify the Agency's Chief Executive Officer of its determination.

4. Upon receipt of the Human Subjects Committee's approval, the program management shall decide whether or not to proceed with the research project. If the program management decides to participate in the research, program management will ensure that ongoing reports are provided to the Human Subjects Committee for monitoring purposes.

CONSENT FOR TAKING AND FOR USE OF PHOTOGRAPHS/ VIDEOTAPE

POLICY NO. 14

POLICY

The Agency seeks to ensure that photographs and/or videotapes of its clients are taken only after obtaining consent from the clients.

PROCEDURES

1. When a request is made by Agency Staff to photograph or videotape a client or clients for Agency purposes, the Program Manager/Department Director shall ensure that the Agency's standard *Consent for Taking and for Use of Photographs/Videotape* form has been signed by the client, parent or guardian and witnessed by another individual prior to the taking of any photographs or videotape.

2. The original consent form shall be retained in the files of the Agency program/department taking the photograph or videotape. A copy of the consent shall be retained in the client's file.

3. Any requests made by outside parties to photograph or videotape Agency clients, shall be reviewed by the Program Manager/Department Director in consultation with the Office of Development and Communications. If the Program Manager/Department Director and Communications Director determine that such request is reasonable and will not disrupt the program, the Program Manager/Department Director will contact the Agency's Legal Office for its review of any consent forms provided by the outside party.

4. When the outside party's consent form has been approved by the Legal Office, the Program Manager/Department Director shall ensure that the consent form has been signed by the client, parent or guardian and witnessed prior to the taking of any photographs or videotape.

5. A copy of the consent form shall be retained in the client's file.

ETHICAL BEHAVIOR **POLICY NO. 15**

POLICY

Employees shall perform their jobs in accordance with the professional standards of their position, the Agency's Code of Ethics and Best Practices, the Agency's Standards of Conduct and other Agency policies and procedures.

PROCEDURES

Employees shall:

1. Carry out their jobs/provision of services in a manner that demonstrates a commitment to honesty, integrity and compliance with the law.

2. Familiarize themselves with the Compliance Program's Standards of Conduct and Compliance Program policies and procedures.

3. Review and understand the key policies governing their particular job/service functions.

4. Report any fraud, abuse or other improper activity through the mechanisms established under the Compliance Program.

5. Cooperate in Agency audits and investigations.

6. Maintain a pleasant and efficient work environment and treat fellow employees, clients and visitors courteously, professionally and with respect. In times of conflict, employees shall adhere to this same Standards of Conduct and shall follow Agency policies and procedures on how to resolve conflicts.

7. Maintain confidentiality at all times. Employees may only divulge confidential information on a need to know basis when authorized to do so.

Employees shall perform their jobs in accordance with the professional standards of their position, the Agency's Code of Ethics and Best Practices.

PROCEDURES

Employees shall adhere to the following:

1. Maintain a pleasant and efficient working environment. Treat fellow employees, clients and visitors courteously, professionally and with respect. In times of

conflict, employees shall adhere to this same Standards of Conduct and shall follow Agency policies and procedures on how to resolve conflicts.

2. Confidentiality must be maintained at all times. Employees may only divulge confidential information on a need to know basis when authorized to do so.

CORPORATE COMPLIANCE AS JOB RESPONSIBILITY POLICY NO. 15A

PURPOSE

The Agency relies on its employees and other affected individuals' good faith participation in and cooperation with the Compliance Program in order to make the Compliance Program effective. The purpose of this policy is to ensure that all employees and other affected individuals are aware of their responsibilities in the area of Corporate Compliance.

POLICY

Participation in and cooperation with the Compliance Program is a job responsibility of employees and a service responsibility of other affected individuals. Supervisors will consider employees' performance in the area of Corporate Compliance during the employees' Annual Performance Evaluation. For other affected individuals, their performance in the area of Corporate Compliance will be considered when reviewing their ongoing relationship with the Agency.

PROCEDURES

1. Employees and other affected individuals will familiarize themselves with the Compliance Program's compliance issues, expectations, compliance program operations Standards of Conduct; Mission Statement; Code of Ethics; Best Practices and Compliance Program Policies and Procedures.

2. Employees and other affected Individuals will review and understand the key policies governing their particular job/service responsibilities.

3. Employees and other affected individuals will comply with all laws, rules and regulations, and Agency policies and procedures.

4. Employees and other affected individuals will not engage in fraud, abuse or other non-compliant, unethical or illegal behavior or otherwise violate the Compliance Program Policies and Procedures or any other Agency policies and procedures

5. Employees and other affected individuals will promptly report any compliance issues including fraud, abuse or other improper activities or wrongdoings through the mechanisms established under the Compliance Program (See Compliance Policy 19, *Whistleblower/Reporting Non-Compliance*):

    - notifying their supervisors, directors, vice presidents, or senior vice presidents;
    - notifying the Compliance Office; or
    - filing a report through the Compliance Hotline

6. Employees and other affected individuals will not encourage, direct, facilitate or permit non-compliant behavior.

7. Employees and other affected individuals will assist in the resolution of compliance issues by cooperating with all Agency and government audits and investigations and will participate in and cooperate with any corrective action plans.

8. Employees and other affected individuals will complete all on-line Corporate Compliance trainings in a timely manner and will attend any live trainings or other trainings as mandated by the Agency.

9. Employees and other affected individuals will carry out their job/service responsibilities in a manner that demonstrates a commitment to honesty, integrity and compliance with the law.

10. Employees who fail to comply with any of their Compliance Program job responsibilities will be subject to disciplinary action in accordance with the Agency's *Employee Policy Manual* (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*). Other affected individuals who fail to comply with the Compliance Program may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

11. No employee shall be disciplined solely because he/she in good faith reported what was reasonably believed to be an act of wrongdoing or a violation of the Compliance Program or reported to appropriate officials as provided in Sections 740 and 741 of the New York State Labor Law (see Compliance Policy 19A, *Non-Retaliation/Non-Intimidation)*.

DISCIPLINE **POLICY NO. 15B**

PURPOSE

The Agency relies upon employees and other affected individuals' good faith participation in and cooperation with the Compliance Program. The purpose of this policy is to ensure that all employees and other affected individuals are aware of the disciplinary measures the Agency may take for noncompliance with the Agency's Corporate Compliance Program, improper/illegal activities relating to the Compliance Program, Agency policies and procedures, standards of conduct, or State and Federal laws, rules and regulations.

POLICY

All employees and other affected individuals are expected to comply with all laws, rules and regulations, as well as all provisions of the Agency's Corporate Compliance Program and other Agency policies and procedures. Failure to do so may result in disciplinary action in accordance with the Agency's Personnel Policies and Procedures for employees or termination of role/relationship with Agency, for other affected individuals.

Disciplinary action will be administered on a fair and equitable basis, appropriate to the seriousness of the violation and consistent with the Agency's *Employee Policy Manual*. Enforcement of disciplinary action will be consistent across all Agency job positions and responsibilities.

PROCEDURES

1. Employees will be evaluated for compliance as part of their Annual Performance Evaluation. Factors to be considered are the compliance responsibilities set forth in Compliance Policy 15A, *Compliance as Job Responsibility.*

2. Employees who participate in or engage in fraud, abuse or other non-compliant, unethical or illegal behavior or otherwise violate the Compliance Program Policies and Procedures or any other Agency policies and procedures will be subject to disciplinary action as set forth in the Agency's *Employee Policy Manual*. Discipline may take the form of progressive discipline or summary discharge, depending on the seriousness of the violation. Intentional or reckless behavior will be subject to more significant discipline.

   Other affected individuals who participate in or engage in fraud, abuse or other non-compliant, unethical or illegal behavior or otherwise violate the

Compliance Program Policies and Procedures may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

3. Employees who fail to report fraud, abuse or other non-compliant, unethical or illegal behavior when observed will be subject to disciplinary action as set forth in the Agency's *Employee Policy Manual*, with disciplinary action subject to any applicable collective bargaining agreements. Discipline may take the form of progressive discipline or summary discharge (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*), depending on the seriousness of the violation.

   Other affected individuals who fail to report fraud, abuse or other non-compliant, unethical or illegal behavior when observed may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

4. Employees who encourage, direct, facilitate or permit non-compliant behavior will be subject to disciplinary action as set forth in the Agency's *Employee Policy Manual*, with disciplinary action subject to any applicable collective bargaining agreements. Discipline may take the form of progressive discipline or summary discharge (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*), depending on the seriousness of the violation.

   Other affected individuals who encourage, direct, facilitate or permit non-compliant behavior may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

5. Employees who fail to assist in the resolution of compliance issues by failing to cooperate with Agency and government audits and investigations or by failing to participate in and cooperate with any corrective action plans will be subject to disciplinary action as set forth in the Agency's *Employee Policy Manual*, with disciplinary action subject to any applicable collective bargaining agreements. Discipline may take the form of progressive discipline or summary discharge (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*), depending on the seriousness of the violation.

   Other affected individuals who fail to assist in the resolution of compliance issues by failing to cooperate with Agency and government audits and investigations or by failing to participate in and cooperate with any corrective action plans may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

6. No employee shall be disciplined solely because he/she in good faith reported what was reasonably believed to be an act of wrongdoing or a violation of the Compliance Program or reported to appropriate officials as provided in Sections 740 and 741 of the New York State Labor Law (see Compliance Policy 19A, *Non-Retaliation/Non-Intimidation)*.

USE OF AGENCY RESOURCES AND FUNDS **POLICY NO. 15C**

PURPOSE

The Agency seeks to ensure that Agency resources and funds, whether received from funding sources or other sources, are used appropriately and consistent with the Agency Mission, funding source rules and regulations and all applicable laws.

POLICY

1. Prohibited Uses of City, State and/or Federal Funding

   Consistent with law and funding source regulations, the Agency prohibits the use of City, State and/or Federal funding for activities involving worship, religious instruction, and proselytization. Agency outreach efforts will not discriminate based on religion, religious beliefs, refusal to hold a religious belief or refusal to participate in a religious practice.

2. Using Agency Resources Exclusively for Agency Business

   Employees and other affected individuals shall use the Agency's resources solely for the purpose of carrying out their job responsibilities. The Agency's facilities, equipment, staff and other assets may not be used by an employee or other affected individual for personal benefit or to engage in any outside business or volunteer activity without the prior approval of the Compliance Officer. Employees may not use their affiliation with the Agency to promote any business, charity or political cause. Employees shall seek reimbursement for expenses only to the extent such expenses have been incurred in the course of carrying out their job duties and in accordance with the Agency's expense reimbursement policies.

3. Using the Agency's Resources Exclusively for Charitable Purposes

   The Agency is a tax-exempt organization under Section 501(c)(3) of the Internal Revenue Code which requires the Agency to engage in only those activities that are within its approved charitable purpose. Employees and other affected individuals may not use the Agency's resources to engage in any activity that is outside the scope of the Agency's charitable purpose.

CORPORATE COMPLIANCE TRAINING AND EDUCATION **POLICY NO. 16**

POLICY

It is the policy of the Agency to provide training and education regarding the Corporate Compliance Program to the Compliance Officer, employees and other affected individuals. Such training shall include training on the compliance issues, expectations, compliance program operations, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the False Claims Act (FCA). The Agency will ensure that the Compliance Officer has sufficient training on compliance issues through attendance at outside conferences, subscriptions to trade periodicals and other means.

PROCEDURES

1. All employees and other affected individuals of the Agency will be made aware of the Corporate Compliance Program through the following forums:

- Initial Hire – Employees and volunteers will sign the HIPAA Confidentiality and Security Agreement.

- Program Orientation – All new employees and volunteers will receive initial Corporate Compliance training, including compliance issues, expectations, compliance program operations, HIPAA and FCA, as it relates to their programs/departments. The training will occur within 30 days of hiring.

- Agency Wide Orientation – The Corporate Compliance Program will be referenced at the time of the employee's Agency wide orientation.

- On-line training via the Corporate Compliance website: Staff will receive ongoing training over the course of each year. Ongoing training will include information about any new or amended compliance issues, compliance expectations, compliance program operations, laws, rules, regulations, and policies including those relating to HIPAA and FCA. Ongoing training also will include re-training in existing laws, rules, regulations and policies including those relating to HIPAA and FCA.

- Training for other affected individuals within 30 days of the time they commence their relationship with the Agency.

- Annual training for the Compliance Officer, employees and other affected individuals.

2. The training and education shall include the following topics:

    - The Agency's risk areas and organizational experience;
    - The Agency's written policies and procedures;
    - The role of the Compliance Officer and the Compliance Committee;
    - How employees and other affected individuals can ask questions and report potential compliance-related issues to the Compliance Officer and senior management, including the obligation of affected individuals to report suspected illegal or improper conduct and the procedures for submitting such reports; and the protection from intimidation and retaliation for good faith participation in the compliance program;
    - Disciplinary standards, with an emphasis on those standards related to the Agency's Compliance Program;
    - How the Agency responds to compliance issues and implements corrective action plans;
    - Requirements specific to the Medicaid program and the Agency's services, where applicable;
    - Coding and billing requirements and best practices, if applicable;
    - Claim development and the submission process, if applicable;
    - The Corporate Compliance Office will determine whether it is necessary to develop a curriculum of advanced Corporate Compliance training for a particular program/department.

3. Training and education shall be provided in a form and format accessible and understandable to all affected individuals, consistent with Federal and State language and other access laws, rules or policies.

4. The Agency shall develop and maintain a training plan. The training plan shall, at a minimum, outline the subjects or topics for training and education, the timing and frequency of the training, which affected individuals are required to attend, how attendance will be tracked, and how the effectiveness of the training will be periodically evaluated.

5. Corporate Compliance Program training is mandatory for all staff. Upon completion of the initial Corporate Compliance Training, each employee shall sign the Acknowledgement of Corporate Compliance Training. The Acknowledgment shall be maintained in each employee's personnel file in the Office of Human Resources. Employees shall acknowledge their participation in ongoing training as directed by the Corporate Compliance Office.

Failure to comply with this policy may lead to disciplinary action up to and including termination of employment (See Employee Policy 23, *Progressive Discipline* and Policy 24, *Employee Conduct).*

6. All Board members will receive Compliance Training at the time they join the Board and periodic training thereafter, as needed.

7. Other affected individuals will receive Compliance training within 30 days of the commencement of their relationship with the Agency and periodic trainings thereafter, as needed.

EMPLOYEE CONFLICT OF INTEREST POLICY **POLICY NO. 17**

POLICY

All employees must maintain the integrity of the Agency at all times. Employees may not engage in any activity that would enable them or a relative to benefit financially or otherwise from their association with the Agency. Relative is defined as an employee's spouse or domestic partner, child, parent, sibling, grandparent, grandchild, aunt, uncle, cousin, in-law, step relative or any person living in the household.

All employees must disclose any conflict of interest, potential conflict of interest or appearance of a conflict of interest to the Agency.

PROCEDURES

Employees shall adhere to the following:

1. Employee shall not engage in any activities which constitute a conflict of interest. Employees and/or their relatives may not benefit directly or indirectly from any contracts, transactions, professional services, referrals or leases, entered into by the Agency.

2. Employees may not receive payment or any type of benefit or kickback for referring clients to another provider of services. In addition, employees may not refer clients to their own or a family member's practice or other business.

3. Employees may not perform work or services for another organization if these activities create a conflict of time or interest with their job responsibilities.

4. No employee may hold a position in which he/she supervises or manages a relative or in which an employee could influence a relative's employment, promotion, salary or other management or personnel actions. No related employees may work in the same program, department or program site (See Employee Policy 39, *Employment of Relatives*.)

5. Employees shall disclose any conflict of interest, potential conflict of interest or appearance of a conflict of interest to their immediate supervisors. The supervisor shall refer the matter to the Agency's Legal Office for Executive review and resolution.

6. As a condition of employment, each employee must complete and sign an acknowledgement stating that the employee fully understands his/her obligations

under this policy and acknowledges his/her commitment to comply with the policy as an employee of the Agency.

7. Employees who fail to comply with this policy will be subject to disciplinary action as set forth in the Agency's *Employee Policy Manual* (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*).

BOARD CONFLICT OF INTEREST **POLICY NO. 18**

POLICY

I. PURPOSE AND POLICY

The purpose of the conflicts of interest policy is to protect the Agency's interest when it is contemplating entering into a transaction or arrangement that might benefit the private interest of an officer or director of the Agency. This policy is intended to supplement but not replace any applicable state laws governing conflicts of interest applicable to nonprofit and charitable corporations.

In addition, no Board member shall be an interested person or receive preferential treatment in the application for or receipt of the Agency's services or engage in any activity which constitutes a conflict of interest with his/her functions, duties and responsibilities with the Agency.

II. DEFINITIONS

1. Agency

Agency means Catholic Charities, Diocese of Brooklyn and all its affiliated corporations.

2. Interested Person

Any director, principal officer, or member of a committee with board delegated powers who has a direct or indirect financial interest, as defined below, is an interested person. If a person is an interested person with respect to the affiliates, he or she is an interested person with respect to all entities in the Agency.

3. Financial Interest

A person has a financial interest if the person, directly or indirectly, through business, investment or family, has—

a. an ownership or investment interest in any entity with which the Agency has a transaction or arrangement, or

b. compensation arrangement with the Agency or with any entity or individual with which the Agency has a transaction or arrangement, or

c. a potential ownership or investment interest in, or compensation arrangement with any entity or individual with which the Agency is negotiating a transaction or arrangement

Compensation includes direct and indirect remuneration as well as gifts or favors that are substantial in nature.

III. PROCEDURES

1. Duty to Disclose

In connection with any actual or possible conflicts of interest, an interested person must disclose the existence and nature of his or her financial interest to the directors and members of committees with board delegated powers considering the proposed transaction or arrangement.

2. Determining Whether a Conflict or Interest Exists

After disclosure of the financial interest, the interested person shall leave the board or committee meeting while the financial interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.

3. Procedures for Addressing the Conflicts of Interest

a. The chairperson of the board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.

b. After exercising due diligence, the board or committee shall determine whether the Agency can obtain a more advantageous transaction or arrangement with reasonable efforts from a person or entity that would not give rise to a conflict of interest.

c. If a more advantageous transaction or arrangement is not reasonably attainable under circumstances that would not give rise to a conflict of interest, the board or committee shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in the Agency's best interest and for its own benefit and whether the transaction is fair and reasonable to the Agency and shall make its decision as to whether to enter into the transaction or arrangement in conformity with such determination.

4. Violations of the Conflicts of Interest Policy

a. If the board or committee has reasonable cause to believe that a member has failed to disclose actual or possible conflicts of interest, it shall inform the member of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.

b. If, after hearing the response to the member and making such further investigation as may be warranted in circumstances, the board or committee determines that the member has in fact failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

IV. RECORDS OF PROCEEDINGS

The minutes of the board and all committees with board delegated powers shall contain-

a. the names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the board's or committee's decision as to whether a conflict of interest in fact existed.

b. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection therewith

V. ANNUAL STATEMENTS

Each director, principal officer and member of a committee with board delegated powers shall annually sign a statement which affirms that such person-

a. has received a copy of the conflicts of interest policy,

b. has read and understands the policy,

c. has agreed to comply with the policy, and

d. understands that the Agency is a charitable organization and that in order to maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes

VI. PERIODIC REVIEWS

To ensure that the Agency operates in a manner consistent with its charitable purposes and that it does not engage in activities that could jeopardize its status as an organization exempt from federal income tax, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

a. Whether compensation arrangements and benefits are reasonable and are the result of arm's-length bargaining.

b. Whether partnership and arrangements with service organizations conform to written policies, are properly recorded, reflect reasonable payments for goods and services, further the Agency's charitable purposes and do not result in inurement or impermissible private benefit.

c. Whether agreements to provide care and agreements with other providers, employees, and third party payors further the Agency's charitable purposes and do not result in inurement or impermissible private benefit.

VII. USE OF OUTSIDE EXPERTS

In conducting the periodic reviews provided for above the Agency may, but need not, use outside advisors. If outside experts are used their use shall not relieve the board of its responsibility for ensuring that periodic reviews are conducted.

WHISTLEBLOWER/REPORTING NON-COMPLIANCE **POLICY NO. 19**

POLICY

The Agency requires employees and other affected individuals to comply with all laws, rules, regulations and Agency policies and procedures. In addition, the Agency expects employees and other affected individuals to report any wrongdoings or violations of the Compliance Program by others. As a condition of employment, an employee must sign an acknowledgment stating that the employee understands his/her obligations under this policy. Reporting of a wrongdoing or compliance violations shall never be the basis for a retaliatory action (see Compliance Policy 19A, *Non-Retaliation/Non-Intimidation*). Wrongdoings include but are not limited to:

- Stealing
- Fraud
- Falsifying records
- Misusing premises
- Misusing equipment
- Failure to report any of the above

PROCEDURES

1. Employees and other affected individuals must report immediately any fraud, abuse, falsification of records, misuse of premises or equipment, other wrongdoings or violations of laws, rules, regulations or Agency policies and procedures through one of the following mechanisms established under the Compliance Program:

a. Notifying supervisors, directors, vice presidents or senior vice presidents;

b. Notifying the Compliance Office:

Via mail: 191 Joralemon Street, 3rd Floor, Brooklyn, NY 11201;
Via email: corporatecompliance@ccbq.org; or
Via phone: (718)722-6086/6237

c. Filing a report through the Compliance Hotline at 1(800)493-8330. Affected Individuals have the option of leaving an anonymous message or leaving their names with a message. It is essential that the employee or affected individual provide sufficient information to investigate the wrongdoing. A person's identity will be kept confidential unless the matter is subject to a disciplinary proceeding, referred to, or under investigation by, New York State Attorney General Medicaid Fraud Control Unit, New York State Office of Medicaid Inspector General or law enforcement, or

disclosure is required during a legal proceeding. Such person shall be protected under the Agency's policy for non-intimidation and non-retaliation (see section 6 below and Compliance Policy 19A, *Non-Retaliation/Non-Intimidation*).

2. Employees, supervisors, directors, vice presidents or senior vice presidents who receive reports under this policy should refer the matter to the Compliance Office.

3. The Compliance Officer will acknowledge receipt of the complaint/wrongdoing where possible within 10 days of receiving a report.

4. The Compliance Office shall review, investigate and ensure that appropriate actions are taken to correct the wrongdoing or compliance violation (See Compliance Policy 40, *Responding to Compliance Issues*).

5. Employees who fail to comply with this policy will be subject to disciplinary action as set forth in the Agency's Employee Policy Manual (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*).

Other affected individuals who fail to comply with this policy may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

6. No employee, director, officer or other affected individual who in good faith reports any action or suspected action that is illegal, fraudulent or in violation of any Agency policy shall be subject to intimidation, harassment, discrimination or other retaliation. No employee shall be subject to an adverse employment action solely because the employee in good faith reported what was reasonably believed to be an act of wrongdoing, a violation of the Compliance Program or reported to appropriate officials as provided in Sections 740 and 741 of the New York State Labor Law. See also Compliance Policy 19A, *Non-Retaliation/Non-Intimidation*.

7. The Agency has designated the Compliance Officer to act as administrator of this policy. The Compliance Officer shall report any actions taken pursuant to this policy to the Board of Trustees/Directors or designated committee, provided that directors who are employees may not participate in any deliberations or voting relating to the administration of this policy.

8. An individual subject to a complaint under this policy shall not be present at or participate in any deliberations or vote on any matter relating to such complaint. However, the Board of Directors may request that the individual present information or answer questions prior to deliberations or vote on the matter.

9. A copy of the policy shall be distributed to all employees and other affected individuals who provide substantial services to the Agency. Distribution for these purposes may include posting the policy on the Agency's website or at the Agency's office in a conspicuous location accessible to employees and other affected individuals.

NON-RETALIATION/NON-INTIMIDATION **POLICY NO. 19A**

POLICY

The Agency relies on its employees and other affected individuals to report suspected fraud, abuse or any other violations of law or Agency policies. A major deterrent to such reporting is the fear of intimidation or retaliation for making the report. The Agency prohibits any form of intimidation or retaliation against employees or other affected individuals for good faith participation in the Corporate Compliance Program, including, but not limited to, reporting potential wrongdoings or issues to appropriate personnel, participating in investigations of potential compliance issues, self-evaluations, audits and remedial/corrective actions, and reporting instances of intimidation or retaliation, including to appropriate officials as provided in Sections 740 and 741 of New York State Labor Law and reporting potential fraud, waste or abuse to the appropriate State or Federal entities.

The types of retaliation that are prohibited include but are not limited to:

- Intimidation;
- Adverse actions with respect to work assignments, salary, vacation or any other terms of employment;
- Unlawful discrimination;
- Termination of employment;
- Threats of any of the above.

An adverse disciplinary action against an employee whose job performance or conduct warrant such actions for reasons unrelated to the reporting of a wrongdoing will not be deemed a violation of this policy.

PROCEDURES

1. Employees and other affected individuals must report immediately all wrongdoings or compliance violations either to a supervisor, director, vice president, senior vice president, the Compliance Office or the Compliance Hotline (see Compliance Policy 19, *Whistleblower/Reporting Non-Compliance*). Employees, supervisors, directors, vice presidents or senior vice presidents who receive reports under this policy should refer the matter to the Compliance Office.

2. An employee who believes he/she has been or is being subjected to intimidation or retaliatory action for good faith participation in the Compliance Program, including, but not limited to, reporting potential wrongdoings or issues to appropriate personnel, participating in investigations of potential compliance issues, self-evaluations,

audits and remedial/corrective actions, and reporting instances of intimidation or retaliation, including to appropriate officials as provided in Sections 740 and 741 of New York State Labor Law and reporting potential fraud, waste or abuse to the appropriate State or Federal entities. should contact the Compliance Office or the Office of Human Resources.

3. The Compliance Office and Office of Human Resources shall apprise each other of receipt of allegations of intimidation/retaliation and shall coordinate the investigation/review of the matter and the issuance of a determination.

4. Employees who violate this policy will be subject to disciplinary action up to and including termination of employment (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct).*

Other affected individuals who fail to comply with this policy may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

PROTECTION OF CLIENT FUNDS POLICY **POLICY NO. 20**

POLICY

Client funds shall be separately maintained and never commingled with Agency or third party funds. As part of the Agency's fiduciary responsibility for client funds, it will exercise good faith and be fully accountable for all payments on the client's behalf. Any deductions from client funds shall be made in accordance with funding source rules and regulations and Agency Fiscal Office guidelines. All programs must establish written protocols to ensure compliance with this policy.

PROCEDURES

1. Each program manager shall maintain a list of all clients for whom the program acts as a fiduciary. Client monies must be maintained in separate accounts. Withdrawals from these accounts must be done in a manner that will sufficiently record and indicate why and how the monies were spent. A proper accounting system must be established at each program.

2. Each program manager shall maintain a list of all clients from whom the program receives money for program fees and expenses. After deductions for a client's personal allowance, the Program may deduct established fees for services.

3. Any employee who becomes aware of a breach of this policy should refer to Compliance Policy 19, *Whistleblower/Reporting Non-Compliance* and take the appropriate action.

POLICY

The Agency is committed to preventing fraud and abuse and to complying with applicable federal and state laws related to fraud and abuse. The Agency's Compliance Program addresses fraud and abuse prevention in policies requiring compliance training, compliance audits, and reporting of compliance issues as well as policies providing whistleblower protections and prohibiting retaliation (this list is not exhaustive).

The Deficit Reduction Act of 2005 requires organizations which receive payments through federally funded programs such as Medicaid and Medicare to provide education to its employees and other affected individuals regarding the federal False Claims Act and state laws that address fraud, waste, abuse and whistleblower protections for reporting such wrongdoings. This policy has been adopted to provide False Claims Act information to employees and other affected individuals.

It is the policy of the Agency to require all employees and other affected individuals to report all known or suspected violations of the Federal False Claims Act ("FFCA") or the New York State False Claims Act ("NYSFCA").

Federal False Claims Act

The federal False Claims Act (the "FCA") is a federal law (31 U.S.C. § 3279) that is intended to prevent fraud in federally funded programs such as Medicare and Medicaid. The FCA makes it illegal to knowingly present, or cause to be presented, a false or fraudulent claim for payment to the federal government. Under the FFCA, the term "knowingly" means acting not only with actual knowledge but also with deliberate ignorance or reckless disregard of the truth.

The federal government may impose harsh penalties under the FFCA. These penalties include "treble damages" (damages equal to three times the amount of the false claims) and civil penalties of up to $11,000 per claim. Individuals or organizations violating the FFCA may also be excluded from participating in federal programs.

<u>Examples of Potential FCA Violations</u>

Examples of the type of conduct that may violate the FCA include the following:

- Knowingly submitting claims to the Medicaid program for services not actually rendered or for which the Agency is otherwise not entitled to reimbursement;
- Knowingly submitting inaccurate, misleading or incomplete Medicaid reports; and
- Knowingly failing to seek payment from other insurers or government

programs that provide coverage to a client before billing Medicaid.

The FCA's Qui Tam Provisions

The FCA contains a *qui tam* or whistleblower provision that permits individuals with knowledge of false claims activity to file a lawsuit on behalf of the federal government. These individuals are referred to as "relators." The relator's lawsuit is filed under seal, which means it is kept confidential until the U.S. Justice Department reviews the case and decides whether to take over prosecution of the matter. An individual is considered a relator only if he or she is the "original source" of the report to the federal government. An individual is not the original source if the report involves activities that are already the subject of a government investigation or have previously been disclosed by the provider to the government. If a relator's lawsuit is successful, the relator may receive a share of the award, plus reasonable expenses and attorneys' fees.

The FCA's Whistleblower Protections

The FCA prohibits retaliation against employees for filing a *qui tam* lawsuit or otherwise assisting in the prosecution of an FCA claim. Compliance Policy 19, *Whistleblower/Reporting Non-Compliance* and Compliance Policy 19A, *Non-Retaliation/Non-Intimidation* strictly prohibit any form of retaliation or intimidation against employees for filing or assisting in any reporting of wrongdoing.

New York State False Claims Act

The New York State False Claims Act or NYSFCA (New York State Finance Law, Chapter 56, Article XIII) is similar to the FFCA. The law prohibits the filing of false or fraudulent claims for payment against any state of local government. The law covers an array of wrongdoing from health care fraud to fraud involving any type of government contract. Under the NYSFCA, civil penalties range from $6,000 to $12,000 per claim plus treble damages.

New York State False Claims Act Qui Tam Provisions

As with the FFCA, an individual acting on behalf of the government (relators) can bring an action under the NYSFCA. If the case concludes with payments back to the government, the relator may recover part of the proceeds.

New York State False Claims Act Whistleblower Protections

Under the NYSFCA, any employee who is discharged, demoted, suspended, threatened, harassed or in any other manner discriminated against in the terms and conditions of employment because of lawful acts by the employee on behalf of the employer or others in furtherance of an action under the NYSFCA, shall be entitled to all relief necessary to make the employee whole.

PROCEDURES

1. Employees and other affected individuals should report any claim or report that appears to be false or fraudulent, or any other conduct that appears to violate the federal False Claims Act or New York State False Claims Act.

2. Employees and other affected individuals may make such reports through any of the mechanisms described in Compliance Policy 19, *Whistleblower/Reporting Non-Compliance*. All reports received will be evaluated and investigated as necessary pursuant to such policy. Employees and other affected individuals are encouraged to contact supervisors or the Compliance Officer if they have questions as to whether certain practices violate the FFCA or NYSFCA.

4. While employees have the legal right to file *qui tam* lawsuits and the Agency will not impede an employee from filing such a lawsuit or retaliate against the employee, employees are encouraged to report and attempt to resolve suspected FFCA or NYSFCA violations through the internal procedures established by the Agency prior to filing such a case.

5. Employees who violate this policy may be subject to disciplinary action up to and including termination of employment (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct).*

Other affected individuals who fail to comply with this policy may be subject to termination of their role with the Agency, depending on the severity of the non-compliance.

AUDITING AND MONITORING **POLICY NO. 22**

POLICY

The Agency shall establish and implement an effective system for the routine monitoring and identification of compliance risks. The system shall include internal monitoring and audits and, as appropriate, external audits, to evaluate the Agency's compliance with the requirements of the Medicaid program and the overall effectiveness of the Agency's compliance program. Audits shall cover such areas as billing, record keeping, internal controls, HIPAA privacy and security regulations and adherence to other laws, rules and regulations as well as the Agency's policies and procedures.

PROCEDURES

1. Auditing

The Compliance Office shall have routine audits conducted by internal or external auditors who have expertise in state and federal Medicaid program requirements and applicable laws, rules and regulations, or have expertise in the subject area of the audit. Audits or investigations conducted by state or federal governmental entities are not considered external audits for purposes of this paragraph. The audits required shall meet the following requirements:

A. Internal and external compliance audits shall focus on the following risk areas:

(1) billings;
(2) payments;
(3) ordered services;
(4) medical necessity;
(5) quality of care;
(6) governance;
(7) mandatory reporting;
(8) credentialing;
(9) contractor, subcontractor, agent or independent contract oversight
(10) other risk areas that are identified by the Agency through its organizational experience.

B. The results of all internal or external audits, or audits conducted by the State or Federal government of the Agency, shall be reviewed for risk areas that can be included in updates to the Agency's Compliance Program and Compliance Work Plan.

C. The design, implementation, and results of any internal or external audits shall be documented, and the results shared with the Compliance Committee and the Governing Body.

D. Any Medicaid program overpayments identified shall be reported, returned and explained in accordance with the provisions of 18 NYCRR Part 521-3 and the shall promptly take corrective action to prevent recurrence.

2. Annual Compliance Program Review

The Agency shall develop and undertake a process for reviewing, at least annually, whether the requirements of 18 NYCRR Part 521 have been met. The purpose of such reviews shall be to determine the effectiveness of the Compliance Program, and whether any revision or corrective action is required.

A. The reviews may be carried out by the Compliance Officer, Compliance Committee, external auditors, or other staff designated by the Agency, provided however, that such other staff have the necessary knowledge and expertise to evaluate the effectiveness of the components of the Compliance Program they are reviewing and are independent from the functions being reviewed.

B. The reviews should include on-site visits, interviews with affected individuals, review of records, surveys, or any other comparable method the Agency deems appropriate, provided that such method does not compromise the independence or integrity of the review.

C. The Agency shall document the design, implementation and results of its effectiveness review, and any corrective action implemented.

D. The results of annual Compliance Program reviews shall be shared with the Chief Executive, Senior Management, Compliance Committee and the Governing Body.

3. Excluded Providers

The Agency shall confirm the identity and determine the exclusion status of affected individuals.

A. In determining the exclusion status of a person, the Agency shall review the following State and Federal databases at least every thirty (30) days:
   - New York State Office of the Medicaid Inspector General Exclusion List;
   - Health and Human Services Office of Inspector General's List of Excluded Individuals and Entities.

B. The Agency shall require contractors to comply with the provisions of this paragraph.

4. The results of the activities required by this policy shall be promptly shared with the Compliance Officer and appropriate Compliance personnel.

CLIENTS' RIGHTS	POLICY NO. 22A

POLICY

The Agency ensures the rights and dignity of all clients. Each program must have a Clients' Rights Statement. The Clients' Rights Statement must be posted at the program and given to each client.

PROCEDURES

1. Each program must have a Client's Rights Statement informing clients of their rights and responsibilities. Each statement must inform the client, at a minimum, of the following:

a. That services are provided in a fair and equitable manner
b. That services are provided in a non-discriminatory manner
c. That the Agency will provide sufficient information for a client to make an informed choice about using Agency services.
d. That the client will be informed of the Agency's expectations in return for its services
e. That the client is advised of the hours of operation
f. That the client is advised of the rules and regulations of the program and how a client may be discharged
g. That the client is informed how to file a grievance and provided with contact information within and without the Agency (State Authority)
h. That the client is advised that the Agency serve minors in certain circumstances without parental consent (see Compliance Policy 3, *Serving Minors Without Parental Consent*)
i. That the client is advised that he/she must provide relevant information as a basis for receiving treatment (*Privacy Notice of Information Practices*)
j. That the client is advised that the Agency will ensure, to the best of its ability, that all clients understand oral and written communications and that the Agency will provide the necessary tools, such as an interpreter, for such communications
k. That the client is advised that he/she has the right to request a review of his/her case and that the client can refuse treatment (see Compliance Policy 4, *Client's Right to Refuse Treatment or Services*)
l. That the client is advised of the cost of services
m. That the Agency will protect the confidentiality and privacy of all clients with exceptions as outlined in the *Privacy Notice of Information Practices.*

2. The Clients' Rights Statement must be posted at each program and must be given to each client. An acknowledgement of the receipt of the Clients' Rights Statement, signed and dated by the client or guardian, should be placed in the client's file.

CLIENT GRIEVANCE **POLICY NO. 22B**

POLICY

The Agency ensures that there is a means for clients to express and resolve grievances both within and without the Agency.

PROCEDURES

1. Each Program must prominently display a *Client Bill of Rights* pertinent to the program including procedures for a client/guardian to express and resolve a grievance. At a minimum, the procedures must advise the client/guardian of the following:

a. That a client/guardian has the right to file a grievance both within and without the Agency, free of interference or retaliation

b. How to file a grievance

c. That an independent investigation will be conducted in a timely manner

d. That notification of the resolution will be provided to the client/guardian in writing

e. That a means of appeal is available to the client/guardian if the client/guardian is not in agreement with the resolution

f. That the client/guardian may file a grievance outside the Agency and the process for doing so.

GENERAL COMPUTER USE **POLICY NO. 23**

POLICY

This policy is designed to provide guidelines for the use of all computing devices (e.g. desktops, laptops, tablets, and smartphones) on the Agency's network. Access to the Agency's computer system ("the System") is provided for business use only. Users of the System must observe the controls and behaviors mandated to maintain the confidentiality, integrity and availability of the System, network, and data. This policy applies to all employees, volunteers, consultants, and any other persons working on the System ("users").

PROCEDURES

1. Agreement

All users of the System are required to sign the *Confidentiality Agreement*, or a *Business Associate's Agreement*, and/or similar confidentiality language within a signed vendor agreement. The Compliance and IT Departments will determine the appropriate level of agreement required based on the type of access being requested. All activity on the System is subject to monitoring and therefore, users should have no expectation of privacy when using the System. Users also must be familiar with and comply with all security policies.

2. User Access

System users will be provided with a User ID and password. Users may not share their User IDs or passwords with others and users must protect their passwords. Passwords must conform to Policy 24, *User Password*. Any suspected breaches must be reported to the IT Helpdesk immediately.

3. Computer Access

The IT Department will provide equipment to users. Users must obtain prior approval from the IT Department for access to the network for any equipment not owned and managed by the System. The equipment must have proper anti-malware software installed and updated with the latest signatures. The attachment of unauthorized equipment to the network (wired or wireless) is prohibited.

4. Shared Responsibility for System Security

It is the shared responsibility of all users to maintain the security of the System. The IT Department will provide periodic security alerts via email, pop ups, bulletins or training. In order to maintain a secure environment, the IT Department will scan and identify system vulnerabilities and send updates and patches to users. At times, users may be prompted to accept or acknowledge a planned patch or update.

5. Desktop Security

When leaving their computers, users shall sign off or lock their computers to prevent other users from accessing the machines. When using a shared workstation, users must sign off at the completion of their sessions. For computers in vulnerable locations, a screen saver must be activated after a brief period of inactivity in order to prevent unauthorized viewing.

6. Antivirus/Anti-Malware

Deterring computer virus infections or other malicious attacks is critical to ensuring the confidentially, integrity and availability of the System. Therefore, updated anti-malware software must be running on every computer accessing the System. Users should report any suspicious activity to the IT Help Desk immediately. Disabling System anti-malware software is prohibited.

7. Using Anti-Malware Software

All Agency e-mail is scanned for viruses. In order to avoid downloading a virus, users should not open executables or command files if unsure of the program's source or purpose.

8. Hacking

Users are prohibited from engaging in any harmful computer activities including, but not limited to, the following:

- Development of any form of computer virus or malicious code fragment;
- Intentional distribution of a virus, worm, Trojan, etc.;
- Creation of false alarms using hoax virus messages, chain mail or spam;
- Downloading or installing any unlicensed or malicious software programs or hacker utilities (such as network sniffers, scanners, password cracking programs, etc.) onto any computer that may be attached to the System network;

- Intentional corruption of software programs or data to make them unusable or invalid;

- Intentional tampering or changing software programs or data from their original form in a manner that violates their integrity and trustworthiness;

- Creation or use of "back doors" or other system workarounds which have the intent or effect of bypassing System security procedures or controls;

- Any unapproved or unauthorized modification or reconfiguration of applications installed by the System.

9. Computer Data

Users are prohibited from viewing, copying, moving, modifying or storing any information unrelated to their work tasks and/or job responsibilities. This prohibition especially applies to any data or content which may be considered protected health information (PHI) or proprietary business information (PBI) or any information considered confidential in nature. The IT Department must be notified immediately if sensitive information unrelated to users' official assignments and/or job responsibilities is accessed or modified unintentionally or if intentional, unauthorized access is suspected. Adequate security measures must be taken to ensure security of all System data stored on computers or media, regardless of location.

10. Backup of Computer Data

The IT Department is responsible for the safeguarding of all servers and networked storage. Safeguarding includes backing up the network shared drives, shared applications and system data that reside on hardware in the computing centers. Users should store all data on their network home drives or department shared drives only. Only business related data should be backed up and stored. Users are responsible for backing up data on their local PC or laptop.

11. Managing Sensitive Data

All users are responsible for protecting the confidentiality, integrity and availability of PHI and PBI as required by law and accreditation requirements. When not in use, PHI/PBI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured. When PHI/PBI is being released electronically (e.g. e-mail), users must protect the PHI/PBI by restricting access to authorized personnel only. PHI/PBI stored on diskettes, CD-ROM, USB drives or other removable data storage media must be protected with strong encryption and should not be commingled with other electronic information. USB drives with appropriate

security controls and strong encryption must be used. Disposable media must be destroyed when no longer required. Removing sensitive data from Agency premises is prohibited unless authorized by a manager or Agency contact for other users and each such occurrence must be logged.

12. Remote Access

Remote access is available for authorized employees and approved third party users. The use of remote access to the System Network is a privilege intended to assist and enhance normal business functions and is subject to all requirements of this Policy as well as all other Security policies. Access to applications is at the discretion of management and may require additional authorization.

13. Prohibited Behavior

Users are prohibited from:

- Loading personal software onto System computers without prior approval from their Department/Program Manager or Agency contact and IT Department;
- Downloading or installing any programs that are shared on the Internet or made available free of charge (Freeware and Shareware);
- Reconfiguring, in any way, the security Applications installed by the IT Department;
- Using file sharing software such as LimeWire, Morpheus, Bit Torrent, etc.;
- Pirating software or copyrighted material, including installing software without sufficient licenses, copying DVDs, and "loaning" copies of software to others;
- Changing the configuration of computer hardware configuration without consulting the IT Department (e.g. modems, storage devices, printers).

14. Printers

Network and local printers are provided for System users to perform necessary work-related functions. Although printed documents are sometimes necessary, users are encouraged to make their work environment as "paperless" as possible. When confidential electronic information needs to be printed, the paper copies must be treated with an appropriate level of confidentiality and security, and disposed of when no longer needed in accordance with Agency policies and procedures.

15. Wireless Devices

Users must contact the IT Help Desk to request authorization before connecting their wireless devices to the System's private wireless network. Unauthorized wireless devices and/or access points are strictly forbidden and are subject to immediate disconnection from the System's private wireless network. Users connecting to the System's wireless network are responsible for understanding and following requirements outlined in Policy No. 27, *Wireless*, as well as all other Security policies and will be held responsible for any misuse or violation.

16. Physical Security

Users must follow best practices to protect System computers from loss or theft. Office doors should always be locked when an office is unoccupied during off-hours, and during business hours, if practical. Physical relocation of any System computer equipment is prohibited, unless approved and performed by the IT Department. Managers/Agency contacts are responsible for evaluating the need for computer locks and should contact the IT Department for purchase of approved locking devices. Users who work in public areas and have computer monitors that may be viewed by clients or visitors must take precautions to prevent unauthorized persons from viewing computer screens. Managers/Agency contacts are responsible for evaluating the need for monitor privacy screens or changing the location of desks.

17. Security of Mobile Computers

The small size and portability of some computers such as notebook computers, tablet PCs, and personal digital assistants (PDAs), increase the likelihood for such devices to be lost or stolen. Users must take extra care to ensure that sensitive data and confidential information contained on the devices are secure including, but not limited to, the following:

- Employing an enterprise encryption technology to protect stored data;
- Securing access to the device with passwords;
- Never leaving a device unattended in public areas, and storing under lock when not in use;
- Never leaving a device in an unattended vehicle.

Users must immediately report the loss or theft of a computer or mobile device to the IT Department.

18. Enforcement

Users should report any violations of this policy to their Managers/Agency contact. If appropriate, the violation should be escalated and reported to the IT Helpdesk or the Director of IT. Employees who violate this policy may be subject to disciplinary action up to and including termination of employment (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct)*. Other users who violate this policy may be subject to termination of their role with the Agency, depending on the severity of violation.

USER PASSWORD **POLICY NO. 24**

POLICY

Passwords are an important aspect of computer security and serve as a method for protecting the confidentiality, integrity and availability of user accounts and access to the Agency's Information System and networks ("The System").

PROCEDURES

1. Password Standards

The following are minimum requirements for selecting strong passwords for the Agency's System. Systems and applications which cannot support the required lengths and complexity are required to use the strongest settings possible for maximum security, and must be reported to the IT Department as exceptions.

a. Passwords shall be a minimum of 7 characters in length for users, and a minimum of eight characters in length for users with elevated privileges (e.g., system and network administrators).

b. Passwords should contain at least three of the following characters:

i. Lower case alphabetic [a - z];
ii. Upper case alphabetic [A - Z]
iii. Numeric [0 – 9]
iv. Special Character [!@#$%^&*()_+|~-=\`{}[ ]:";'<>?,./]

c. All network user passwords expire after 90 days. Any user whose password has expired must change his/her password before completing the login process and gaining access to computer/network resources. A password that is expired for more than 90 days will cause the associated User ID to be disabled.

d. Multiple consecutive failed login attempts within a given amount of time will result in a user's account being locked. The user must contact the IT Helpdesk to address this situation.

2. Maintaining Password Integrity

a. All passwords shall be treated as sensitive, confidential information, and should not be shared with anyone, including administrative assistants. If account access needs to be granted to additional employees or other users, the supervisor/Agency contact must submit a Service Request to the IT Helpdesk.

b. Passwords should never be written down or stored on-line unless appropriately secured or encrypted.

c. Users shall not use the same or similar passwords for Agency accounts as for other non-Agency access (e.g., home e-mail account, websites, benefits, etc.).

d. Users should never use the "Remember Password" feature of applications (e.g., Outlook, browsers).

3. Assigning Passwords

A supervisor/Agency contact is responsible for arranging the initial assignment of a password to a new user by sending a written request to the IT Department. At the time of termination of a user's employment or relationship with the Agency, the supervisor/Agency contact is responsible for notifying the IT Department in writing of the termination.

MULTI-FACTOR AUTHENTICATION **POLICY NO. 24A**

POLICY

In an effort to maintain the confidentiality and privacy of Agency stakeholders, and in order to protect Agency systems against hacking, the Agency requires that all users access Agency systems by using multi-factor authentication (where such technology has been enabled). Multi-factor authentication (MFA) is a method for providing increased security when accessing computer resources whereby the multiple authentication factors include 'Something you know', such as a PIN, used in conjunction with 'Something you have', such as a security token.

PROCEDURES

1. RSA MFA and Unique Security Tokens

The Agency has selected RSA as the primary MFA solution which ensures that "you *are* you" by assigning users' computer accounts a unique security token, in either hard or soft token versions.

a. Users who have been issued an Agency smartphone are eligible to use the RSA soft token version, also known as Secure ID, which can be installed as an app on the Agency smartphone.

b. Users who do not have Agency smartphones may elect to either use their own smartphones for the RSA soft token version (Secure ID) or to use a hard token version issued by the Agency.

2. Accessing Systems with RSA MFA

In order to access systems protected with RSA MFA, users will be required to:

a. When prompted, enter their Agency username.

b. When prompted, enter their multi-factor authentication information.

c. When prompted enter their Agency or system password.

3. Maintaining Token Integrity

All tokens shall be treated as sensitive, confidential information and should not be shared with anyone, including other users. Users should contact the IT Department if technical assistance is needed. Tokens should be maintained in a secure manner at all times, by remaining with the user while at work and being safely stored at the user's home during non-working hours.

4. Lost or Stolen Tokens

If a token is lost or stolen the user must immediately contact their supervisor/Agency contact and the IT Department to report the missing or stolen token.

5. Malfunctioning Tokens

Users should contact the IT Department to address any technical issues with their tokens.

6. Returning Tokens

Hard tokens must be returned to the IT Department upon termination.

7. Employee Responsibility for Tokens

Ensuring the availability of a soft or hard token during work hours is a job responsibility of all employees and a requirement for other users in order to access Agency systems where MFA technology has been enabled.

a. Users who elect to use a soft token must ensure that the Agency or personal smartphone installed with the soft token app is with them during work hours and sufficiently charged.

b. Users who elect to use a hard token must ensure that the hard token is with them during work hours.

c. A pattern of failure and/or ongoing failure to comply with this policy by having a token available during work hours or any other failure to comply with this policy may subject an employee to disciplinary action (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct).* Failure to comply with this policy may subject other users to termination of their role with the Agency, depending on the severity of the non-compliance.

E-MAIL/OTHER ELECTRONIC COMMUNICATIONS ACCEPTABLE USE POLICY NO. 25

POLICY

The Agency monitors e-mail content and use for the purposes of, but not limited to, preventing unauthorized access, preventing security breaches and maintaining the confidentiality of data. The Agency e-mail system is for Agency business use and all e-mails are the property of the Agency.

PROCEDURES

1. E-mail Use

Users of the e-mail system should have no expectation of privacy related to their e-mail accounts. While the e-mail system is for Agency business use only, infrequent and minimal personal use of the Agency e-mail system is permitted as allowed by a user's supervisor/Agency, and provided it does not interfere with work duties and responsibilities, is consistent with professional conduct, is not for personal financial gain, and is lawful.

2. E-mail Format

In general, e-mail messages should be constructed so information is clear, concise and cannot be misconstrued. In particular;

a. E-mails should contain a subject line.

b. Subject lines must not contain protected health information (PHI) or proprietary business information (PBI).

c. E-mails should contain a signature block including the following:

- First name and last name
- Title
- Program or department.
- Catholic Charities of Brooklyn and Queens or affiliate name
- Work address
- Telephone number (office and cell) and fax number
- Email address

- Disclaimer (example*: **Please note**: The information in this email, including any attachments, may be privileged and confidential and protected from disclosure. It is intended solely for the addressee. Access to this email by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. Please immediately contact the sender if you have received this message in error and delete the message from your computer. Thank you*.)

3. E-mail Content

E-mail size, including attachments, must not exceed 10MB.

a. E-mails which contain PHI or PBI in the content should be identified in the subject line with the word "Secure" (see below).

b. Users are prohibited from sending e-mails containing the following:

i. Any material, text or speech that violates Agency policies.

ii. Chain e-mail letters or their equivalent.

iii. Solicitations or private business activities.

c. The e-mail system may not be used for any activities deemed unlawful, criminal or immoral.

d. The e-mail system must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

e. Users are prohibited from intentionally sending spam.

f. Users who receive e-mails with content they feel violates the Agency's policies should report the matter to their supervisors or the IT Helpdesk.

4. PHI and PBI

The Agency has a duty to protect the confidentiality, integrity and availability of sensitive data, in particular PHI and PBI, as required by Federal and State law. E-mail may be used to communicate PHI or PBI when necessary for the completion of job functions as follows:

a. Users should determine whether e-mail is the appropriate method to send the PHI or PBI, and, where possible, should avoid using e-mail for highly sensitive PHI or PBI.

b. All e-mails sent to external e-mail systems and which contain PHI or PBI, must be encrypted by including the word "Secure" in the e-mail subject line. E-mail addresses should be confirmed before sending to ensure the e-mail is delivered to the appropriate recipient.

c. The minimum necessary amount of PHI should be included in the e-mail to accomplish the intended purpose.

d. A user must obtain supervisory/Agency contact approval prior to using e-mail or texting as a form of communication with a client (see # 5).

e. In the event that an e-mail containing PHI is delivered to the wrong recipient, the user must immediately notify their supervisor/Agency contact and the Chief Privacy Officer or the Chief Security Officer.

f. Requests for exceptions to these policies must be addressed to the Chief Privacy Officer who may consult with the Chief Compliance Officer to identify a secure alternative for transmission.

g. To ensure all client e-mails conform to the HIPAA Security Rule, written consent from the client must be obtained prior to using e-mail as a form of communication with a client (E-mail/Electronic Communication Consent Form). All e-mail communications with clients or with users concerning client care must be sent through the Agency's e-mail portal and not through standard e-mail services such as AOL, Optimum, Yahoo, Gmail, etc.

5. E-mail Communication with Clients

Users who communicate with clients through the use of e-mail must adhere to the following:

a. All e-mails must conform to all Agency policies.

b. All clients must sign an E-Mail/Electronic Communication Consent prior to initiating e-mail communication.

c. With the exception of appointment scheduling, e-mail communication may only occur with existing clients.

d. E-mail communication with clients should be used only for non-emergency, non-urgent or non-critical information.

e. Copies of all e-mail communications relative to ongoing care of the client must be maintained as part of the client's record. All clinically relevant e-mail communications must be a permanent part of the client's record.

f. E-mail communication with clients or with users concerning client care will be considered and treated with the same degree of privacy and confidentiality as the written client record.

6. Receiving E-mails

a. Unsolicited or unexpected e-mails received from outside or unknown parties should never be opened but rather, should be deleted immediately to prevent unauthorized access to the computer network.

b. Files downloaded from personal e-mail accounts or extracted from inbound messages are checked for malicious attachments. These files could potentially contain viruses, worms or other malicious malware. Unauthorized interception or disclosure of e-mail is prohibited.

7. E-mail Forwarding

Users should exercise caution when forwarding messages.

a. Incoming e-mails should not be auto forwarded to an external e-mail account.

b. Users should never forward suspicious e-mails (potentially virus infected; spoofed messages; unknown recipients; etc.).

8. Mass E-mail Communication to all System E-mail Accounts

a. Only authorized users are permitted to mass email all System e-mail users. A user who needs to mass e-mail all System users must contact the IT Helpdesk in order to obtain authorization.

b. Content of the System wide e-mail must be relevant to the Agency or its employees.

9. E-mail Retention

E-mail systems are not intended for long-term storage of important information.

a. Users are responsible for moving important information from e-mail messages to network drives, personal folders or off-line back-up media.

b. Electronic mail records should be maintained in the same manner as other records and retained in accordance with System procedures.

c. All e-mails older than 180 days should be archived from the user's mail box.

d. Archived e-mail may be purged as needed by storage management, or regulatory or legal requirements.

10. Offline Archiving of E-mails

All e-mails are archived in long-term storage by the IT Department and may be monitored, reviewed and restored at the discretion of management.

11. E-mail for Persons Not Employed by the Agency

In some instances, an e-mail address will be provided to persons not employed by the Agency, such as consultants, independent contractors and volunteers. Use of a System e-mail address by a non-employee shall conform to all of the requirements set forth in this policy.

E-Mail/Electronic Communication Consent

The Agency may use e-mail or other forms of electronic communication, such as texting, to communicate with you about various matters. E-mail and other forms of electronic communication are not completely secure methods of communication: information could potentially be sent to the wrong person, it may not be the most timely method of communication and it is dependent on technology which may or may not work all the time. If you chose to communicate with the Agency via e-mail or other forms of electronic communication, the Agency asks that you acknowledge and consent to the following:

I understand that e-mail communication should not be used for emergencies or for communicating time sensitive information.

I understand that e-mail communication will be processed during routine business hours. In the event I do not receive a response, I understand that I should contact the office directly.

I understand that due to situations outside of the control of the Agency, internet and e-mail service may be interrupted or not work at any given time. The Agency is not responsible for technical failures.

I will not share, distribute, release or sell an Agency e-mail address to anyone.

I understand that e-mail communication is not a substitute for care and evaluation. I must arrange for an appointment to assure appropriate care.

I understand that I am to provide my full name and contact information in all e-mails, e.g., full name, address, phone number(s).

I understand and accept that the Agency may route my e-mail to other members of the staff for informational purposes or for expediting a response. I authorize the Agency to send and to designate staff to receive and read my e-mail.

I authorize the Agency to share the content of my e-mails on a need to know basis, subject to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

E-mails originating from the Agency's computer network will use encryption technologies to prevent interception of e-mails by inappropriate parties. However, I acknowledge that many commonly used e-mail services are not secure and fall outside

the security requirement set forth by HIPAA for the transmission of protected information. Therefore, I understand there is a risk that my health information may be obtained by others not affiliated with the Agency. I authorize the Agency to transmit my personal health information via e-mail even though e-mail may not be secure and private and may be subject to loss or exposure.

I acknowledge and accept that the Agency can terminate e-mail or other electronic communication services at any time.

I understand that I am responsible for notifying the Agency if I chose to discontinue e-mail or other electronic communications or if my e-mail address has changed.

_____
Client/Guardian Signature

_____
Print Name

_____
Date

_____
Relationship if other than client

_____
Witness Signature

_____
Client E-mail Address

INTERNET USE **POLICY NO. 26**

POLICY

The Agency provides employees, volunteers, contractors and visitors ("users") with Internet access through the computer network for the express purpose of performing work-related activities or research. The Agency reserves the right to monitor the use of the Internet by users. Unauthorized use of the Internet is prohibited.

PROCEDURES

1. Users are required to sign the Agency's *Confidentiality Agreement and Acknowledgement Regarding Use of Computers, E-Mail and the Internet* form. Individuals provided with Internet access should be familiar with and adhere to Compliance Policy 23, *General Computer Use* and Compliance Policy 25, *E-mail/Other Electronic Communications Acceptable Use* as well as all Security policies.

2. Internet access is provided to users with the understanding that web-based services can greatly enhance business activities and improve client services. However, some Internet technologies (such as streaming media or webcasts) place significant bandwidth burdens on the Computer Network and will be monitored for abuse. Users utilizing bandwidth intensive web services may only do so outside of normal business hours or with the permission of the IT department.

3. Reasonable personal use of the Internet may be permitted at the discretion of the employee's manager/director. Reasonable personal use includes accessing financial sites, personal research, shopping on-line, etc. Accessing pornographic sites and sites that promote racism, gambling, illegal activities or other inappropriate business material is prohibited.

4. Users are responsible for all activity occurring through their Internet accounts. Users will be held accountable for any costs, charges or purchases incurred via Internet transactions. Users also will be held responsible for criminal activity which includes but is not limited to:

- Distributing pornography or unwanted obscenity, fraudulent or related activity;
- Transmitting script/code that would cause damage;
- Wire fraud, malicious mischief, threat, interception of electronic communication;

- Intellectual property crimes;
- Cyber stalking, harassment, defamation, indecent and abusing e-mails;
- Launching of virus, worms and Trojans;
- Denial-of-service attacks, or illegally accessing information on another computer.

5. Sending and receiving Internet traffic via wireless devices (such as Smartphones, Notebooks, iPads, etc.) also is subject to this policy. Users must contact the IT Helpdesk to request authorization before connecting their wireless device to the Computer Network and enabling Internet access via the device.

6. Internet users are prohibited from disabling anti-malware or firewall protection. Users must exercise care when downloading any material from the Internet, and will be held responsible for copyright violations.

7. The unauthorized use of Peer-to-Peer file sharing software (such as Napster, LimeWire, Morpheus, Bit Torrent, Gnutella, etc.) is prohibited.

8. The Agency may, at any time, determine it is necessary to monitor user activity and filter certain websites or URLs, or completely block access to the Internet. These monitoring, filtering, or blocking actions may be imposed across entire sections of the Computer Network, or may be focused on certain individual users or groups of users.

USE OF AGENCY COMPUTERS/DEVICES FOR AGENCY WORK POLICY NO. 28

POLICY

All work performed by Agency employees during the course of their employment is property of the Agency ("Agency Information"). The Agency is committed to the protection of all Agency Information including client related information. In order to protect Agency Information, employees may only create, store and transmit Agency Information on Agency approved personal computers, laptops or other devices, except where approved in writing by the Chief Compliance Officer, Chief Privacy Officer, or Chief Security Officer. Employees may transfer Agency information off Agency configured servers, personal computers, laptops or other devices and onto non-Agency portable or online media only after obtaining written authorization from the Chief Compliance Officer, Chief Privacy Officer, or Chief Security Officer, and only by using appropriate encryption and password protection*.

PROCEDURES

1. Employees and supervisors shall ensure that all Agency work, including accessing agency email, is conducted on Agency approved personal computers, laptops, portable media, or other devices ("Agency Devices").
   - Examples of portable media and other devices includes, but is not limited to; Smartphones, Tablets (iPads), Laptops, CDs/DVDs, USB Flash Drives, Memory Cards.

2. Employees may not create, transmit, or store data on non-Agency Devices or Online Services (e.g., OneDrive, Dropbox, iCloud, Google Drive, Non-Agency Email such as Gmail or Yahoo) except under the following circumstances and with prior written authorization from a Vice President and the Chief Privacy Officer or the Chief Security Officer;
   - For the purposes of data backup*,
   - For the purpose of exchanging large amounts of data with Business Associates*,
   - For the purpose of continuity of service*.

3. All portable media containing Agency Information must be approved by and obtained from the Information Technology Department. Employees are responsible and accountable for portable media containing Agency Information in their possession.
   [Note: Logging, encryption, Inventory, etc. should be performed by IT]

Employees may not open Agency files or access Agency Data on non-Agency Devices, such as those defined in Procedure 1, except on non-Agency Devices that have been authorized as detailed above. This includes accessing Agency Email.

** (Please refer to the IT department for specific procedures)*

RECEIPT AND RETURN OF AGENCY DEVICES NO. 28A

POLICY

The Agency may provide employees with Agency cell phones, iPads, laptops or other portable devices ("Agency Devices") in order to assist employees with performing their job duties and responsibilities. Agency devices are provided to employees only upon supervisory approval and only through the IT Department. Agency Devices shall remain the property of the Agency at all times.

PROCEDURES

1. Employees shall sign an *Acknowledgment of Receipt of Agency Devices* form when they receive Agency devices.

2. Employees shall conduct Agency work on Agency devices. (See Employee Policy 35, *Use of Agency Equipment and Computer Systems* and Compliance Policy 28*, Use of Agency Computers/Devices for Agency Work*).

3. Employees who are working remotely shall comply with Employee Policy 19, *Flexible Workplace*.

4. Employees shall take good care of Agency devices while in their possession and store them securely when not in use. In the event an Agency device is lost, stolen or damaged in any way, employees must immediately report the matter to their supervisors and to the IT Department by emailing IT helpdesk or calling (718)722-6059.

5. If an employee terminates employment, for any reason, the employee must immediately return the Agency devices to the Agency as set forth below. Employees must sign a *Return of Agency Devices* form when they return Agency devices.
    a. Employees shall return Agency devices in person, as directed by their program/department. Employees who do not return Agency devices as per this policy will not terminate in good standing.
    b. Under exceptional circumstances, an employee who is unable to return the Agency devices in person may contact the supervisor and IT Department to request approval to ship the Agency devices to the Agency.
        - Encrypted IT equipment devices may be returned by this method provided the device login and password information are NOT included with the shipment.
        - Unencrypted IT equipment devices that may have data on them may not be returned by shipping.
        - Employees must contact their supervisors and IT Department to request approval to ship Agency devices to the Agency. Such requests must be approved by the Program/Department management and Legal, Human Resources, and IT Department representatives.

- Employees who have received prior approval to ship Agency devices must follow the Shipping Instructions for Return of Agency Devices.

COMPUTER INFORMATION SYSTEMS SECURITY TRAINING **POLICY NO. 30**

POLICY

The Agency seeks to ensure that its employees are aware of the security issues involved in the use of computer information systems.

PROCEDURES

1. As part of HIPAA Training, the Office of Information Technology offers Computer Information Systems Security Training on the Agency Intranet via the public folders.

2. The training covers the following areas:

   a. Back Up and Contingency Planning
   b. Access and Security Issues
   c. Computer Information Systems Policies
   d. Accessing Technical Support
   e. Retention and deletion of emails and files

3. All new employees using the Agency's computer systems must take the training as soon as possible but no later than thirty (30) days after commencement of employment.

4. All employees must take a refresher course every three years.

5. Program Managers and Department Directors shall conduct additional trainings as necessary for their own programs.

6. As per the HIPAA Training Policy, a signed acknowledgment of training shall be forwarded to the Office of Human Resources for placement in the personnel file.

FAX POLICY **POLICY NO. 31**

POLICY

In order to protect the confidentiality and integrity of confidential information of its clients, the Agency complies with all applicable laws, rules and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), as well as applicable codes of professional ethics.

PROCEDURES

In order to comply with this Policy, all employees must strictly observe the following standards relating to facsimile communications of client records:

1. Employees may transmit confidential client records by facsimile only when urgently needed for client care or required by a third-party payer for ongoing certification of payment.

2. The information transmitted must be limited to that necessary to meet the requester's needs.

3. Except as authorized by law, a properly completed and signed authorization must be obtained before releasing client information (see *Privacy Notice of Information Practices*).

4. Employees may not send by fax sensitive medical information, including, but not limited to, AIDS/HIV information, mental health and developmental disability information, alcohol and drug abuse information, and other sexually transmissible disease information without the express authorization of the Program Manager/Department Director.

5. The Agency's authorized fax cover sheet must be used.

6. Employees must make reasonable efforts to ensure that they send the facsimile transmission to the correct destination. Where possible, employees must preprogram frequently used numbers into the machine to prevent misdialing errors. For a new recipient, the sender must verify the fax number before sending the facsimile and verify the recipient's authority to receive confidential information.

7. Fax machines must be in secure areas and the Program Manager/Department Director is responsible for limiting access to them.

8. Each program/department is responsible for ensuring that incoming faxes are properly handled, not left sitting on or near the machine, and are distributed to the proper recipient expeditiously while protecting confidentiality during distribution.

9. Employees must report any misdirected faxes to the immediate supervisor.

10. All supervisors will periodically check all speed-dial numbers to ensure their currency, validity, accuracy, and authorization to receive confidential information. The Chief Security Officer will conduct random checks of the speed dial numbers.

11. Employees must immediately report violations of this policy to their immediate supervisor for appropriate corrective or disciplinary action. The immediate supervisor may consult with Human Resources or the Chief Security Officer if necessary.

12. All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct)*.

RETENTION OF RECORDS **POLICY NO. 32**

POLICY

The records of the Agency are important assets. Agency records include client files, corporate documents, personnel files, fiscal records and any documents produced by Agency officers, directors, employees, and consultants in the course of working for the Agency, whether paper or electronic. Records can take many forms including, but not limited to: case notes, memoranda, emails, contracts, computerized calendars, voicemail, appointment books and expense records.

The Agency is required to maintain certain types of records for specified periods of time. All employees must comply with the record retention schedule attached to this policy as Appendix A and any updated schedules provided at later times.

The Agency also is required to comply with provisions of the Sarbanes-Oxley Act of 2002 which prohibits the alteration, cover up, falsification, or destruction of any document to prevent its use in an investigation or official proceeding. The Agency may suspend the destruction of records to comply with this law.

PROCEDURES

1. Storage of Records

Records must be stored in a safe and secure manner so as to minimize risk of loss, damage or tampering and should be accessible only to authorized employees, consultants or volunteers. Records shall be maintained at the program site or department where they are created unless otherwise directed. All client files and Agency personnel files shall be stored in a secure environment, i.e., in locked cabinets or password protected electronic files.

2. Electronic Documents and Records

Electronic documents shall be retained as if they were paper documents. Any electronic files that fall into one of the document types in Appendix A will be maintained for the appropriate amount of time. In general, email messages should be deleted after one year unless there is sufficient reason to retain them for a longer period of time. If an employee has a sufficient reason to keep an email message, the message should be printed in hard copy and kept in the appropriate file or, preferably, moved to an “archive” computer file folder.

3. Client Records

All client records shall be retained as per Appendix A. If a closed case is reopened, then later closed, the retention period shall commence anew. If client cases have been closed for the retention period and retention of the file is not feasible or necessary, the records may be destroyed. Minors' records shall be stored for a minimum of seven (7) years after the age of 18. If a closed case is reopened, then later closed, the seven (7) year time period shall commence anew. Destruction of client records shall occur only upon the authorization of a Vice President. If a client file is to be destroyed, the program shall maintain a record of basic information: the client's name, date of birth, social security number if known, program of service and dates of service. Such basic information shall be retained for an indefinite period of time.

4. Personnel Files

Personnel records of employees who have been terminated for ten (10) years or more may be destroyed. Destruction of records shall occur only upon the authorization of the Director of the Office of Human Resources. If a personnel record is to be destroyed, the Office of Human Resources shall maintain a record of basic information: the employee's name, date of birth, social security number, and dates of employment. Such basic information shall be retained for an indefinite period of time

5. Correspondence and Internal Memoranda

Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration).

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. Correspondence pertaining to routine matters and having no significant, lasting consequence should be discarded after one year.

6. Suspension of Record Destruction in the Event of Litigation or Claims

No employee shall destroy, dispose of, cover up, or alter any document or record while knowing that it is or may be relevant to an anticipated or ongoing investigation or legal proceeding conducted by or before a federal, state or local government agency, including tax and regulatory agencies, law enforcement agencies, and civil and criminal courts, or an anticipated or ongoing internal investigation, audit or review conducted by the Agency.

If an employee believes or if the Agency informs an employee that Agency records are relevant to litigation or an investigation, then the records must be preserved and

destruction of the records shall be suspended until such time as the Office of Legal Affairs determines the records are no longer needed.

Appendix A – Record Retention Schedule

File Category	Item	Retention Period
Client Records	Case files	7 years after case closed or funding source minimum, whichever is longer. *Basic information to be retained. See Procedures #3.
	Minors' case files	After case is closed, 7 years after the age of 18. *Basic information to be retained. See Procedures #3.
	Incident Reports	10 years
Corporate Records	Bylaws and Certificates of Incorporation	Permanent
	Corporate resolutions	Permanent
	Board and committee meeting agendas and minutes	Permanent
	Conflict-of-interest disclosure forms	7 years
	Licenses and permits	Permanent
	Sales Tax Exemption letters	Permanent
	Senior Team meeting minutes	3 years
	Agency Strategic Plans	7 years after expiration
	Organization Charts	7 years
Contracts	Contracts and agreements and related correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination
Corporate Compliance	Hot line complaint log Investigations	7 years 7 years
Correspondence	General (including email) Legal and important matters	1 year Permanent
Development And Communication	Records of Contributions	Permanent

	Other documents evidencing gifts	Permanent
	Fundraising files	6 years
	Press clippings, TV/Radio/Video transcripts	6 years
	PR related photos	6 years
	Press releases	10 years
	Advertising	6 years
	Agency publications including brochures	6 years
Finance and Administration	Annual Audit Reports and Financial statements (audited)	Permanent
	Annual Audit Records, including work papers and other documents that relate to audit	7 years
	Auditor management letters	7 years
	Annual plans and budgets	7 years
	Check register and checks	7 years
	Bank deposits and statements	7 years
	Chart of accounts	7 years
	General ledgers	Permanent
	Investment performance reports	7 years
	Equipment files and maintenance records	7 years after disposition
	Accounts payable ledgers and schedules	7 years
	Accounts receivable legers and schedules	7 years
	Notes receivable ledgers and schedules	7 years
	Investment records	7 years after sale of investment
	Credit card records	2 years
	Tax bills, receipts, statements	7 years
Insurance Records	Policies	7 years after expiration
	Certificates of Insurance	Active plus 7 years
	Accident reports	7 years
	Safety (OSHA) reports	7 years
	Claims (after settlement)	7 years
	Group disability records	7 years after end of benefits

Legal	Legal Memoranda and Opinions (including all subject matter files)	7 years after close of matter
	Litigation files	6 years after case closed
	Court orders	Permanent
	Estate Files	6 years
	Requests for departure from Records Retention Plan	10 years
Real Estate	Deeds	Permanent
	Leases (expired)	7 years after all obligations end
	Mortgages, security agreements	7 years after all obligations end
Tax	IRS exemption determination and related correspondence	Permanent
	IRS rulings	Permanent
	IRS Form 990s	Permanent
	Tax returns – Income, Franchise, Property	Permanent
	Tax work paper packages	7 years
	Sales/Use Tax records	7 years
Human Resources	Employee personnel files, Payroll records and Attendance records	10 years from date of termination *Basic information to be retained. See Procedures #4.
	Retirement plan benefits (plan descriptions, plan documents)	Permanent
	Employee handbooks	Permanent
	Workers' Compensation claims (after settlement)	7 years
	Employee orientation and training materials	7 years after use ends
	Employment applications and resumes (non-employees)	1 year

	IRS Form I-9 (store separate from personnel file)	3 years after date of hire or 1 year after termination, whichever is later
	Withholding tax statements	7 years
Technology	Software licenses and support agreements	7 years after all obligations end
Miscellaneous	Consultant reports	2 years
	Annual Reports	Permanent
	Material of historical value (including pictures, publications)	Permanent
	Policies and Procedures Manuals	Current version with revision history

CONTROLS FOR PHYSICAL ACCESS TO AGENCY PREMISES POLICY NO. 33

POLICY

The Agency seeks to ensure that all Agency premises are safeguarded from unauthorized physical access, tampering and theft.

PROCEDURES

1. Each Program Manager/Department Director shall devise a facility security plan to safeguard the interior and exterior portions of the program/department as well as the equipment contained therein from unauthorized physical access, tampering and theft.

2. The facility security plan shall include the following:

   a. Procedure to ensure that all exterior doors to the facility are secured, consistent with fire codes, at all times except when monitored by an employee, volunteer or security guard during business hours.

   b. Procedure for identifying employees, clients and visitors to the premises prior to entry.

   c. Procedure for signing in and out visitors and providing escorts through the premises if deemed necessary by the Program Manager/Department Director.

   d. Procedure for ensuring that all doors are locked and any alarms activated when the program/department is closed for business at the end of the day.

3. The facility security plan shall be reviewed and approved by the Program Manager/Department Director's supervisor. All employees at the program/department shall be made aware of the approved plan and the approved plan shall be posted in an appropriate location.

CONTINUOUS QUALITY IMPROVEMENT **POLICY NO. 34**

POLICY STATEMENT

As part of the Agency's commitment to the delivery of quality services, the Agency requires all programs to engage in an ongoing quality improvement process. Each division (or sub-division) must implement an annual Continuous Quality Improvement (CQI) Plan and submit periodic updates. All CQI Plans must be congruent with the requirements of program funding sources, regulatory bodies, and Agency strategic directions.

PROCEDURE

1. Each division (or sub-division) will identify a Continuous Quality Improvement (CQI) Committee which may meet as a stand-alone committee or be incorporated as part of regular management meetings.

2. The CQI Committee must meet no less than once each quarter.
    a. Minutes of the meetings must be kept.
    b. If part of regular management meetings, a section of the meeting minutes must clearly identify CQI discussion.

3. The CQI Committee is responsible for the development, implementation and monitoring of the Annual CQI Plan.

4. The Annual CQI Plan includes:
    a. The membership of the division's (or sub-division's) Quality Improvement Committee
    b. The intended goal(s) of the improvement actions
    c. The source that identified the goal(s)
    d. The measure by which improvement will be assessed
    e. The programs that will be involved in the plan

5. Update reports are required at mid-year and at the end of the fiscal year. These reports include for each goal:
    a. The dates of CQI Committee meetings during the reporting period
    b. The actions taken during the reporting period
    c. The results of the actions taken
    d. The next steps in improving the focus area
    e. Ad-hoc quality improvement actions

6. Annual CQI Plans and CQI Updates are to be submitted to a designee in the Office of Planning and Evaluation.

7. The Office of Planning and Evaluation will provide each division (or sub-division) with templates for assistance in the development of both the Annual CQI Plan and CQI Update Reports.

8. The Office of Planning and Evaluation will create an annual CQI Report using the information provided in the Annual CQI Plan and the CQI Update Reports.

9. The annual report will be shared with each division so that successful actions can be replicated as applicable across the Agency.

10. The annual report will be submitted by the Office of Planning and Evaluation to the Corporate Compliance Office, the CCNS Board of Directors and the Planning Committee of the CCBQ Board of Trustees.

USE OF AGENCY'S ATTORNEYS — POLICY NO. 35

POLICY

The agency seeks to ensure that all programs and departments comply with the laws, rules and regulations pertaining to the various services of the Agency.

PROCEDURES

All programs and departments should contact the attorneys for the Agency for any advice and guidance in matters of a legal nature. Such matters include but are not limited to the following examples: Leasing, contracting, purchase of services agreement, letters of agreement, request for client documents, etc.

1. Programs and departments should ensure that they follow all policies and procedures in relation to requests for client documents, confidential information containing records, etc. If in doubt in relation to any policy concerning a legal matter, staff should consult the Agency's attorneys.

2. All summonses and complaints should be directed to the Office of Legal Affairs at 191 Joralemon Street, Brooklyn, NY 11201.

3. All subpoenas that are served at programs, should be brought to the attention of the Agency's attorneys.

4. Accidents, injuries, fires and floods on Agency leased or owned premises should be reported to the Office of Legal Affairs and the Insurance Office.

5. No records of any kind should be provided on a verbal request without prior consultation with the Office of Legal Affairs.

6. All requests for employee records or information should be directed to the Office of Human Resources which shall consult with the Office of Legal Affairs as necessary (see Employee Policy 61, *Employee Information Requests*).

CONTRACTING STANDARDS **POLICY NO. 36**

POLICY

In order to ensure compliance with the Agency's mission and purpose, applicable laws and in order to protect the Agency from liability, the Agency will ensure that all Agency contracts, memoranda of understanding (MOU) and letters of agreement (LOA) comply with contracting standards as set forth in this policy.

PROCEDURES

1. Prior to entering into a contract with a contractor, the Agency will ensure that all bidding requirements, as set forth by the program's funding source and/or the Agency's Fiscal Office, have been followed and that the contractor has been screened, where appropriate, as set forth in Compliance Policy 37, *Contractor Selection*.

2. The Agency shall not enter into a contract, MOU or LOA with any entity or person in violation of Compliance Policy 17, *Employee Conflicts of Interest* or Compliance Policy 18, *Board Conflicts of Interest*. If an employee becomes aware that the Agency has entered into or is contemplating entering into a contract, MOU or LOA in violation of such policies, the employee will immediately notify the Compliance Office.

3. Employees shall not accept gift or gratuities of any kind from vendors or prospective vendors of the Agency. Gifts include the provision of any item or service at less than fair market value. The only exception to this prohibition is that employees are permitted to accept unsolicited gifts of nominal value (e.g., candy during the holiday season) from existing vendors of the Agency. If an employee is unsure whether a gift from a vendor violates this policy, the employee shall contact the Compliance Office for clarification.

4. Employees shall not solicit or receive anything of value from a vendor or other organization (a kickback), in violation of the Agency's *Code of Ethics* and Compliance Policy 17, *Employee Conflicts of Interest*, even if such item is for the benefit of the Agency. This prohibition does not apply to discounts offered by vendors on their products or services.

5. Agency contracts, MOUs and LOAs shall contain certain standard terms and conditions including, as appropriate, the following:

   a. Roles and responsibilities of the parties
   b. Duration of the contract/agreement
   c. Services to be provided
   d. Clearly defined performance goals and measurable outcomes

e. Payment terms
f. Procedures for sharing information
g. Insurance requirements
h. Indemnification
i. Language specifying that the contractor is subject to the Agency's Compliance Program to the extent that the contractor is affected by the Agency's risk areas and only within the scope of the contracted authority and affected risk areas.
j. Contractor assurances that it is not engaged in fraud, abuse or improper activities
k. Conditions for termination, including termination for failure to adhere to the Agency's Compliance Program requirements

6. All contracts, MOUs and LOAs entered into by the Agency must be reviewed and approved by the Office of Legal Affairs prior to execution. Contracts, MOUs and LOAs shall be executed only by designated officers/signatories of the Agency. The Office of Legal Affairs or its designee will maintain a database of all Agency contracts, MOUs and LOAs for tracking and monitoring purposes.

7. Employees will promptly notify the Compliance Office if they become aware of any suspected fraudulent, abusive or other illegal activity by a contractor. The Compliance Office or designated personnel shall investigate the matter and determine whether the contractor has engaged in improper conduct. The Agency will promptly terminate the contract of any contractor that has been found to have engaged in fraudulent, abusive or other illegal activity.

8. All records relating the implementation of this policy, including but not limited to, documents evidencing the screening, supervision and termination of contractors shall be maintained for six years.

9. Failure to comply with this policy may lead to disciplinary action up to and including termination of employment (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct*).

CONTRACTOR SELECTION **POLICY NO. 37**

POLICY

In order to ensure compliance with applicable laws and to protect the Agency from liability, the Agency does business only with reputable and law abiding contractors and subcontractors. The Agency shall not enter into a contract unless the contractor has been screened in accordance with this policy.

PROCEDURES

1. Prior to entering into a new contract, the Agency's Central Purchasing Department will conduct a reference check to determine whether the contractor is reputable and trustworthy. The reference check will consist of contacting at least two other companies with which the contractor has done business. A reference check may be waived for a start-up company without sufficient prior experience or other unusual circumstances.

2. Upon completion of a satisfactory reference check, the Purchasing Department, where required in accordance with Compliance Policy 22, *Auditing and Monitoring*, will screen the potential contractor and any individuals who own 10% or more of a corporate entity against the U.S. Department of Health and Human Services Office of Inspector General's List of Excluded Individuals/Entities, New York State Office of the Medicaid Inspector General Exclusion List and any other exclusion list as may be required. The Agency shall not contract with any individual or entity who is included on these lists at the time the contract is being proposed. The Agency shall confirm the identity and determine the exclusion status of affected individuals.

3. The Purchasing Department shall screen all existing contractors against the U.S. Department of Health and Human Services Office of Inspector General's List of Excluded Individuals/Entities and New York State Office of the Medicaid Inspector General Exclusion List on a monthly basis. If this screening reveals that a contractor is included on the exclusion lists, the Agency will immediately terminate the contractor's contract.

4. A contractor must obtain Agency approval prior to entering into a subcontract. No subcontract will be approved unless the Purchasing Office screens the subcontractor against the exclusion lists and determines that the subcontractor is not an excluded person.

5. Once a contractor has been screened and approved, the Agency will enter into a contract with the contractor which complies with Compliance Policy 36, *Contracting Standards*.

6. Failure to comply with this policy may lead to disciplinary action up to and including termination of employment (See Employee Policy 23, *Progressive Discipline* and Employee Policy 24, *Employee Conduct)*.

SUPERVISION **POLICY NO. 38**

POLICY

Each Agency supervisor shall provide regular and formal individual supervision to all employees he/she supervises. Supervision must include direction, coordination, productivity enhancement, and an evaluation. All supervision is directed at ensuring the delivery of quality services. Formal supervision forums can include group supervision and staff meetings. "Open door" and "on-the-spot" supervision practices may augment the process but does not replace formal supervision.

PROCEDURES

1. An agenda should be prepared by the supervisor and shared with the employee prior to the supervision meeting. The agenda should focus on job duties, responsibilities, and work assignments. Supervisory sessions are to include discussion and guidance to employees on the following:

    a. Mission and best practices guidelines
    b. Agency policies and procedures
    c. Delegation and oversight of work assignments
    d. Identifying training needs
    e. Contractual requirements

2. The supervisor must document the supervision meeting and should include at minimum but not limited to:

    a. Consultation
    b. Constructive criticism concerning developmental needs of employees and training to improve skill levels.
    c. Praise
    d. Annual Performance Appraisal Goals

3. All supervision documentation must be maintained in the employee's file in the program/department

BREACH NOTIFICATION **POLICY NO. 39**

POLICY

The Agency will investigate and provide notice of a breach of unsecured protected health information (PHI) to affected individuals and/or Federal and State agencies in accordance with applicable Federal and State laws, rules and regulations.

Definition of Breach

A breach notification is required when a breach of unsecured PHI has occurred. Unsecured PHI is PHI that is not encrypted or has not been otherwise physically destroyed (by shredding, etc.). A breach is defined as an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the Agency demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

Exceptions to the Definition of "Breach"

1. The unintentional, good faith access or use of PHI by a workforce member or business associate.
2. The inadvertent disclosure of PHI within the Agency or a business associate.
3. A good faith belief that the unauthorized person would not have been reasonably able to retain the information.

Breach Notification Requirements

In the event of a breach of unsecured PHI, the Agency will provide notification of the breach to affected individuals, the Secretary of Health and Human Services (HHS), and, in certain circumstances, to the media. In addition, business associates must notify the Agency if a breach occurs at or by the business associate.

1. Individual Notice

Individual notice will be provided in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If there is insufficient or out-of-date contact information for 10 or more individuals, substitute individual notice will be provided either by posting the notice on the home page of the

Agency web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The Agency will include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the Agency has insufficient or out-of-date contact information for fewer than 10 individuals, it may provide substitute notice by an alternative form of written notice, by telephone, or other means.

The individual notifications will be provided without unreasonable delay and not later than 60 days following the discovery of a breach and will include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Agency is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the Agency (or business associate, if applicable).

With respect to a breach at or by a business associate, while the Agency is ultimately responsible for ensuring individuals are notified, the Agency may delegate the responsibility of providing individual notices to the business associate. The Agency and business associates will consider which entity is in the best position to provide notice to the individual, by considering various circumstances, such as the functions the business associate performs on behalf of the Agency and which entity has the relationship with the individual.

2. Media Notice

If the Agency experiences a breach affecting more than 500 residents of a State or jurisdiction, in addition to notifying the affected individuals, it will provide notice to prominent media outlets serving the State or jurisdiction. The Agency may provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

3. Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), the Agency will notify the Secretary of the US Department of Health and Human Services (HHS) of breaches of unsecured PHI by completing and electronically submitting a breach report form to the HHS website. If a breach affects 500 or more individuals, the Agency will notify the Secretary without unreasonable delay and in no case later than 60 days following the breach. If a breach affects fewer than 500 individuals, the Agency may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

4. Notification by a Business Associate

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the Agency following the discovery of the breach. A business associate must provide notice to the Agency without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate must provide the Agency with the identification of each individual affected by the breach as well as any other available information required to be provided by the Agency in its notification to affected individuals. Upon notification by the business associate of discovery of a breach, the Agency will be responsible for notifying affected individuals, unless the Agency and business associate agree that the business associate shall notify the affected individuals.

Delay of Notification Authorized for Law Enforcement Purposes. If a law enforcement official notifies the Agency that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Agency shall:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

This provision applies to notices made to individuals, the media, HHS, and by business associates.

Maintenance of Breach Information. The Agency shall a maintain record of all breaches of unsecured PHI, regardless of the number of individuals affected. The following information will be collected for each breach:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.
- A description of the types of unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address, other).
- A description of the action taken with regard to notification of individuals regarding the breach.
- Steps taken to mitigate the breach and prevent future occurrences.

PROCEDURES

7. Employees must report immediately any breaches or potential breaches of PHI to a supervisor, director, vice president, senior vice president or the Compliance Office.

8. Supervisory staff who receive reports of breaches or potential breaches shall refer the matter to the Compliance Office.

9. The Compliance Office shall review and evaluate the matter to determine whether a breach has occurred and shall ensure that any required notifications are made in conformance with this policy and applicable law.

10. The Compliance Office shall document its evaluation and determination of whether a breach occurred as well maintain a record of confirmed breach information and notification.

RESPONDING TO COMPLIANCE ISSUES **POLICY NO. 40**

POLICY

The Agency is committed to promptly responding to compliance issues, including fraud, abuse, or other improper activities identified through internal auditing and monitoring, investigations, reports by employees and other affected individuals or other means.

The Compliance Office is responsible for:

- ensuring compliance issues are investigated;
- reporting compliance issues to outside authorities if appropriate, including but not limited to the New York State Department of Health, New York State Office of Medicaid Inspector General and United States Department of Health and Human Services; and
- ensuring that all necessary corrective actions are taken with the goal of reducing the potential for recurrence of non-compliant behavior; and
- ensuring ongoing compliance with State and Federal laws, rules and regulations, and requirements of the MA program.

PROCEDURES

1. Upon the detection of potential compliance risks and compliance issues, whether through reports received, or as a result of the auditing and monitoring, the Compliance Office shall take prompt action to ensure investigation of the conduct in question and determine what, if any, corrective action is required, and likewise promptly implement such corrective action.

2. The Compliance Office shall document the investigation of the compliance issue which shall include any alleged violations, a description of the investigative process, copies of interview notes and other documents essential for demonstrating that the Agency completed a thorough investigation of the issue. Where appropriate, the Agency may retain outside experts, auditors, or counsel to assist with the investigation.

3. The Agency shall document any disciplinary action taken and the corrective action implemented.

4. If the Agency identifies credible evidence or credibly believes that a State or Federal law, rule or regulation has been violated, the Agency shall promptly report such violation to the appropriate governmental entity, where such reporting is otherwise required by law, rule or regulation. The Compliance Officer shall receive copies of any reports submitted to governmental entities.

5. If the alleged violation involves potential criminal or significant civil liability, the Compliance Office shall notify the appropriate outside authorities for investigation where necessary and/or direct an internal investigation.

6. After review of the investigation report, the Compliance Office shall promulgate actions to resolve confirmed compliance problems, with the goal of reducing the potential for recurrence of non-compliant behavior. Such corrective actions may include, but not be limited to, any of the following:

    - Modifying the Agency's existing policies, procedures or business practices;
    - Providing additional training or other guidance to employees or other affected individuals;
    - Seeking interpretive guidance of applicable laws and regulations from government agencies;
    - Disciplining employees or terminating other affected individuals;
    - Notifying law enforcement authorities of criminal activity by employees or other affected individuals;
    - Returning overpayments or other funds to which the Agency is not entitled to the appropriate government agency or program; or
    - Self-disclosing fraud or other illegality through established state and federal self-disclosure protocols.

    The Compliance Office shall require a report from staff charged with carrying out the corrective actions, confirming that the corrective actions have been implemented or undertaken. The Compliance Office shall set forth an appropriate time schedule, given the nature of the confirmed compliance problem, for production of such reports. The Compliance Office will monitor the effectiveness of implemented corrective action plans in order to reduce the potential for a recurrence of non-compliant behavior.

7. If the investigation reveals evidence of significant Medicaid overpayments, fraud, waste or abuse or other compliance issues related to the Agency's billing under the Medicaid Program, the Compliance Office shall evaluate the appropriateness of reporting such compliance issues to the New York State Department of Health and/or the New York State Office of Medicaid Inspector General (OMIG) pursuant to OMIG's *Medicaid Self-Disclosure Guidance*.

    Issues appropriate for disclosure may include, but are not limited to:

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

8. If the investigation reveals a breach of unsecured protected health information, the Agency will provide notice to affected individuals and/or Federal and State agencies in accordance with applicable Federal and State laws, rules and regulations (Compliance Policy 39, *Breach Notification*).

9. The Compliance Office shall advise the Agency's Chief Executive Officer of all allegations and outcomes of investigations except in the event of a matter involving the Chief Executive Officer in which case the Compliance Officer shall directly report to the Audit Committee of the Board of Trustees.

COMPLIANCE PROGRAM REVIEW **POLICY NO. 41**

POLICY

The Agency is committed to ensuring that its Compliance Program is effective and up to date with applicable laws, rules and regulations.

PROCEDURE

The Agency shall review the Compliance Program written policies and procedures, and standards of conduct at least annually to determine:

1. if such written policies, procedures, and standards of conduct have been implemented;

2. whether the policies, procedures and standard of conduct are available, accessible, and applicable to all affected individuals;

3. whether affected individuals are following the policies, procedures, and standards of conduct;

4. whether such policies, procedures, and standards of conduct are effective; and

5. whether any updates are required.

MEASURING EFFECTIVENESS **POLICY NO. 42**

POLICY

The Board of Trustees of Catholic Charities, Diocese of Brooklyn is committed to undertaking effectiveness assessments to help ensure that there are defined, measurable goals and objectives in place to evaluate the success and impact of the Agency's programs and services in fulfilling these goals and objectives and the Agency's Mission.

PROCEDURES

1. At least once every two years, the Agency will review its goals and objectives toward achieving its Mission and will complete a performance and effectiveness assessment of its programs based upon that review.

2. Such an assessment will be conducted under the authority of the Planning and Evaluation Committee of the Board of Trustees.

3. The Board of Trustees will receive a written report of this assessment:

    a. Describing the activities that the Agency undertook in the prior two years to achieve its goals and objectives;
    b. Identifying the measures used to assess the Agency's effectiveness in achieving its goals and objectives;
    c. Analyzing the effectiveness of the Agency's programs and services in achieving the Agency's goals and objectives;
    d. Recommending future actions the Agency might take to increase effectiveness based on the findings.

4. At the conclusion of this process, the Agency will revise the goals and objectives for the Agency, as needed, for the upcoming term and will suggest means of measuring them.