CATHOLIC CHARITIES OF LONG ISLAND
(Hereafter referred to as Catholic Charities or the Agency)
HIPAA PRIVACY TOOLS
REVISED AS OF JULY 1, 2021; SEPTEMBER 1, 2024, MAY 1, 2025

Privacy Tool #1a:	Corporate Resolutions
Privacy Tool #1b:	Code of Conduct
Privacy Tool #2:	Job Description of the Privacy Officer
Privacy Tool #3:	HIPAA Training Policy
Privacy Tool #4:	Privacy Notice Policy
Privacy Tool #4a:	Privacy Notice
Privacy Tool #4b:	Privacy Notice (in Spanish: Anuncio Confidential de HIPAA)
Privacy Tool #5:	Definitions and Examples of Treatment, Payment and Health Care Operations
Privacy Tool #6:	Disclosures to Family Members, Friends and Personal Representatives Policy
Privacy Tool #7:	Uses and Disclosures of Client Information Policy
Privacy Tool #8:	De-identifying and Re-identifying Client Health Information and Creation of Limited Data Sets Policy including Data Use Agreement
Privacy Tool #9:	Facsimile Transmission of Health Information Policy
Privacy Tool #10a:	Authorization Form for Release of Client Information
Privacy Tool #10b:	Authorization/Consent for Use or Disclosure of Information for Publication Purposes
Privacy Tool #11:	Marketing Policy
Privacy Tool #12:	Fundraising Policy
Privacy Tool #13:	Reserved for Research Policy (Not Used)
Privacy Tool #14:	Client Request Not to Disclose Protected Health Information (PHI) to a Health Plan
Privacy Tool #15:	Minimum Necessary Rule under the Privacy Regulations Policy
Privacy Tool #16:	Uses and Disclosures of Client Information for Various Legal, Public Health, Regulatory and Employment Purposes Policy
Privacy Tool #17:	Access to Client Information and the Right to Amend Client Records Policy
Privacy Tool #18:	Accounting for Disclosures of Client Information Policy
Privacy Tool #19:	Internal HIPAA Complaint and Sanctions for Violations Policy
Privacy Tool #20:	Privacy Hotspots
Privacy Tool #21:	Business Associate Policy
Privacy Tool #21a:	Business Associate Agreement
Privacy Tool #22:	Mitigation
Privacy Tool #23:	Miscellaneous Privacy Rules
Privacy Tool #24:	Procedure to Accommodate Reasonable Requests by Client to Receive Personal Health Information (PHI) By Alternate Means of Communication or At Alternate Location
Privacy Tool #25:	Procedure to Sign in Visitors and Provide Escorts, When Appropriate
Privacy Tool #26:	Record Retention for HIPAA Documentation Policy
Privacy Tool #27:	HIPAA Tool Modification Policy
Privacy Tool #28:	Transcription of Health information Policy
Privacy Tool #29:	Breach Notification (Protected Health Information) Policy
Privacy Tool #30:	Volunteer Confidentiality Agreement Policy
Privacy Tool #31:	Use of Portable Electronic Devices and Remote Access to Information Systems

RESOLUTIONS
OF THE GOVERNING BOARD
OF
CATHOLIC CHARITIES OF THE
DIOCESE OF ROCKVILLE CENTRE

WHEREAS the governing board (the "Board") of Catholic Charities of the Diocese of Rockville Centre (the "Agency"), a New York not-for-profit corporation, is committed to complying with the requirements imposed on the Agency by the administrative simplification provisions of the Federal Health Insurance Portability and Accountability Act of 1996 and its related regulations and standards, as they may be amended from time to time ("HIPAA"); and

WHEREAS it is the collective mission of the Board to ensure the Agency's continuing compliance with HIPAA.

Adopt Compliance Program

NOW, THEREFORE, BE IT RESOLVED, that as a means of evidencing our commitment to compliance with HIPAA, the Agency will develop and implement a compliance program designed to ensure that the Agency meets all applicable requirements of HIPAA; and be it further

RESOLVED, that the Agency shall monitor the development of HIPAA, including, but not limited to, the adoption of new regulations and clarifications of existing regulations, and shall tailor its compliance program on a continuing basis to conform to HIPAA as then in effect; and be it further

Designate a Privacy Officer

RESOLVED, that the Agency hereby creates the position of Privacy Officer. The Privacy Officer will report to the Board regularly on the implementation of the privacy aspects of HIPAA. The Privacy Officer will be accountable for the daily functioning and monitoring of the privacy aspects of the compliance program. The Privacy Officer will implement policies and procedures related to privacy and establish privacy training programs. The Privacy Officer will also be available to assist in responding to any privacy-related violations of HIPAA. The Privacy Officer of the Agency will be designated to the Internal Auditor who will serve at the pleasure of the Board or until his/her successor shall be duly elected and qualified; and be it further

Designate a Security Officer

RESOLVED, that the Agency hereby creates the position of Security Officer. The Security Officer will report to the Board regularly on the implementation of the security aspects of HIPAA. The Security Officer will be accountable for the daily functioning and monitoring of the security aspects of the compliance program. The Security Officer will implement policies and procedures related to security and establish security training programs. The Security Officer will also be available to assist in responding to any security-related violations of HIPAA. The Security Officer will be designated to the MIS Administrator who will serve at the pleasure of the Board or until his/her successor shall be duly elected and qualified; and be it further

Adopt a Code of Conduct

RESOLVED, that the Board hereby adopts the HIPAA Code of Conduct which is attached hereto as Exhibit A; and be it further

Adopt HIPAA Policies and Procedures

RESOLVED, that the Agency shall develop and adopt appropriate policies and procedures related to compliance with HIPAA, and be it further

Purpose

RESOLVED, that the Board's expectation in adopting the foregoing resolutions is that the Agency's HIPAA compliance program will become an established part of the Agency's culture, and will demonstrate its continuing commitment to complying with HIPAA; and be it further

Miscellaneous

RESOLVED, that any and all actions heretofore taken in furtherance of the foregoing resolutions by the officers of the Agency, acting singly be, and hereby are, ratified, approved and confirmed; and be it further

RESOLVED, that each of the officers of the Agency are hereby authorized and empowered to take such steps as such officers may determine to be reasonably necessary, appropriate or advisable to carry out the intent and purposes of the foregoing resolutions, such determination to be conclusively evidenced by the taking of such steps.

IN WITNESS WHEREOF, I have hereunto set my hand as Chair of the Board and affixed the Seal of said Corporation this 17th day of December 2002.

_____

(Msgr.) John Rowan, Chair of the Board

ATTACHMENT A

CODE OF CONDUCT

HIPAA PRIVACY TOOL # 1 b

CATHOLIC CHARITIES
OF LONG ISLAND
(THE "AGENCY")

HIPAA Code of Conduct

As a central part of Catholic Charities of Long Island (the "Agency") HIPAA Compliance Program, this Code of Conduct sets forth the standards of conduct that all personnel of the Agency are expected to follow. Everyone should adhere to both the spirit and the language of this Code in order to avoid any conduct that might violate HIPAA or give the appearance of violating HIPAA.

A. Mission and Values

The Agency is committed to providing clients with quality health care, in a confidential and private manner in accordance with the wishes of its clients and the requirements of applicable law. These standards apply to the Agency's interactions with its clients, other health care providers, consultants, the government entities to whom the Agency reports, public and private third party payers (e.g., Medicare, Medicaid, managed care companies and HMOs), and any other persons and entities with whom the Agency interacts. In this regard, all the Agency personnel and affiliated practitioners must act in compliance with all applicable legal rules and regulations.

The Agency does not, and will not, tolerate any form of unlawful behavior by anyone associated with the Agency. We expect and require all personnel and affiliated practitioners to maintain the confidentiality and security of our clients' health information in accordance with HIPAA standards. To ensure that these expectations are met, the HIPAA Compliance Program will become an integral part of the Agency's corporate mission and business operations.

B. General Standards

1. *Compliance with Applicable Law and Agency Policies*. All personnel and affiliated practitioners are expected to comply specifically with all of the requirements of HIPAA regarding the privacy and security of health information. If personnel and affiliated practitioners are unsure whether a use or disclosure of health information complies with HIPAA, they should bring the matter to their supervisor or the Agency's Privacy or Security Officer.

In addition, all personnel and affiliated practitioners must comply with the policies and procedures developed by the Agency in connection with its HIPAA Compliance Program. Strict compliance with these HIPAA compliance standards is a condition of employment and/or affiliation with the Agency, and a violation of any of these standards of conduct may result in discipline being imposed, which can include termination of employment or professional association, if necessary.

2. *Cooperation with the Compliance Program*. Because of the importance of the HIPAA Compliance Program, we require that each member of the Agency's workforce cooperate fully with this effort. The HIPAA Compliance Program will work effectively only if everyone works together to ensure its success. Therefore, the Agency personnel and affiliated practitioners must understand what is required under the law and this Compliance Program, and must adhere to these standards. In particular, all personnel and affiliated practitioners must cooperate with all inquiries concerning the use, disclosure, transfer, security, release, sharing, utilization, examination, access to, or analysis of an individual's health information and actively work to correct any improper practices that are identified. Furthermore, it is imperative that all personnel and affiliated practitioners report suspected HIPAA violations to their supervisors or to the Privacy Officer or Security Officer or other appropriate high-level officers or administrators of the Agency. Ignoring suspected HIPAA violations may subject personnel to disciplinary proceedings by the Agency.

3. *Retaliation*. The Agency expressly forbids any intimidation, threats, coercion, discrimination or retaliation against individuals who report in good faith suspected HIPAA violations or exercise their rights to health information as provided for by HIPAA.

C. Scope and Application of Standards to Personnel and Others

1. *Personnel Covered.* The Agency's HIPAA Compliance Program, including the standards set forth in this Code of Conduct, applies to all personnel employed by or associated with the Agency and all of its affiliated companies. Each of these entities is fully committed to following the mandates of the Agency's HIPAA Compliance Program, and working with the Agency to ensure mutual compliance with HIPAA. As a result, this Code of Conduct applies to the health care practitioners and personnel of all affiliated entities in the same manner that it applies to the Agency's own personnel and affiliated practitioners.

2. *Contractors and Other Providers.* To the extent practicable, all persons and entities with which the Agency contracts will be asked to cooperate with the Agency's HIPAA Compliance Program. If persons or entities electronically exchange health information with the Agency or receive or disclose health information on behalf of the Agency, then such entities will be required to enter into business associate agreements with the Agency as required by HIPAA. This requirement will apply to, among others, various vendors, and contractors with whom the Agency exchanges health information or who provide services to or on behalf of the Agency. These persons and entities will be encouraged to adopt their own HIPAA Compliance Programs, where appropriate.

HIPAA PRIVACY TOOL #2

CATHOLIC CHARITIES

JOB DESCRIPTION OF THE PRIVACY OFFICER

1. GENERAL DESCRIPTION

   The Privacy Officer is a high-level manager or an officer of the Agency who provides the overall management of the Agency's compliance with HIPAA's Privacy Regulations. The Privacy Officer is responsible for, among other things, implementing the Agency's policies and procedures related to privacy and for establishing privacy education programs.

2. DUTIES AND RESPONSIBILITIES OF THE PRIVACY OFFICER

   The Privacy Officer is responsible for establishing a "culture" of privacy compliance within the Agency. The Privacy Officer must be competent to handle all privacy-related issues as they occur in all sorts of circumstances. Accordingly, the Privacy Officer's role may expand upon unforeseen events and preparing an exhaustive list of his/her responsibilities is impossible. Set forth below are examples of some specific duties of a Privacy Officer:

   A. Providing leadership and setting the agenda for privacy programs and policies.

   B. Supervising and managing the Agency's privacy practices by, among other things, launching audits and investigations when necessary to assure that the confidentiality of client information is maintained by the Agency.

   C. Acting as a liaison with governmental, regulatory, accrediting and other agencies with respect to privacy issues.

   D. Addressing information systems issues relating to the privacy and security of client information and developing appropriate policies and procedures regarding information systems.

   E. Reviewing the business associates who will have access to client information and ensuring that the Agency enters into business associate agreements with them.

   F. Developing and implementing an Agency-wide training program.

   G. Updating the Agency's privacy training programs periodically to assure that all of the employees and agents of the Agency receive appropriate privacy training (including refresher courses, if necessary).

   H. Developing disciplinary and other corrective action procedures to assure that privacy policies are followed.

I. Reporting on the privacy compliance efforts of the Agency to the owners of the Agency or Board in order to assist in the planning, design and evaluation of effective privacy initiatives.

J. Providing strategic guidance to the Agency regarding the privacy and security issues involved in purchases of information technology.

K. Responding to alleged violations of the Privacy Regulations and/or the Agency's privacy policies and procedures.

L. Responding to alleged violations of business associate agreements by the Agency's business associates.

M. Conducting a privacy assessment of the Agency, including all areas of the Agency involved in the flow of client information.

N. Developing the policies and procedures regarding the overall management of client information within the Agency, including, without limitation, policies and procedures regarding the Agency's information safeguards, the Agency's use and disclosure of client information, the Agency's amendment or correction of client information upon client request, the client's right to access, inspect or copy client information, the administrative handling of client information, and the Agency's policies regarding an individual client's request for restrictions and limitations on the disclosure of client information.

O. Providing damage control in the event that client information is wrongfully disclosed by the Agency.

3. SKILLS/EXPERIENCE

The Privacy Officer must be a self-motivated person who can understand privacy issues and implement the multi-faceted privacy policies of the Agency. The Privacy Officer must have good communication skills and must be decisive in order to handle privacy "emergencies." Further, the Privacy Officer should have experience in coordinating activities within the Agency and should have a familiarity with the computer technology that is commonly used in the health system environment. The Privacy Officer must be willing to make changes and enforce the rules even when it makes him/her unpopular and not look for an "easy out." Finally, the Privacy Officer must be aware of the practical cost constraints of the Agency while implementing effective and ethical privacy policies.

HIPAA PRIVACY TOOL #3

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **HIPAA Training**

REFERENCES: **CFR 164.530(b)**

EFFECTIVE DATE: **October 1, 2004; September 1, 2024**

APPROVED BY:

POLICY: In accordance with HIPAA regulations, the Agency will provide training to the entire workforce including employees, volunteers, interns, students, and Board and Committee Members regarding their responsibilities for complying with HIPAA regulations. In addition, independent contractors working in HIPAA covered programs may be trained when determined to be appropriate by the Program Director.

PROCEDURE:
Training may take the form of self-instruction with HIPAA Training Materials, group instruction, or individual instruction. After receiving training, individuals will be required to sign the HIPAA Training Certificate, either manually or online at the Action Center that certifies that they have been trained in confidentiality and HIPAA regulations.

Program Directors are responsible for seeing that all new members of their program's workforce are properly trained in HIPAA Regulations. Training may be provided by management personnel either within the program or at another HIPAA covered program. In addition, training may be offered to all new employees of Catholic Charities of Long Island during each orientation provided by the Human Resources Department.

At the end of the basic level of training, each employee will be required to sign and return the Confidentiality and Training Certification (Privacy Tool #3) either on a hard copy or electronically, Fully executed hard copy certificates will be returned to Human Resources and then filed in Human Resource Files. Electronic documentation signed on the Action Center will be maintained electronuically.

In addition, all employees employed at HIPAA covered programs and those designated independent contractors of HIPAA covered programs will be required to be trained at the Program Level of HIPAA Training offered immediately after the basic level of training.

The Program Director/Administrator is responsible for making sure that all employees of his/her program/department are trained in HIPAA within three months of his/her employment date.

HIPAA training should be continual with reinforcement of Policy and Procedures found in the HIPAA Toolkit at staff meetings for HIPAA covered Programs. The Program Administrator is responsible for ensuring and documenting that this occurs.

Advanced level trainings in the following areas will be given by Department Directors/Administrators/Coordinators. In the event that no one is qualified to train on a particular subject, the advanced level training should be requested of the Privacy Officer who will make arrangements for training of new staff.

Training Module:	**Department**
Information Systems	IT
Fundraising/Marketing	Public Affairs
Human Resources	Human Resources
Business Associates	Directors

HIPAA PRIVACY TOOL #4

CATHOLIC CHARITIES
(the "Agency")

POLICY AND PROCEDURE

SUBJECT: **Privacy Notice**

REFERENCES: **45 CFR §164.502 (i), CFR §164.520**

EFFECTIVE DATE: **October 1, 2004**

APPROVED BY:

Purpose: The Agency is required by law to provide all individuals or their personal representatives a HIPAA compliant Privacy Notice.

Procedure:
Prior to receiving services (except in an emergency or if a client lacks capacity), all individuals (or their personal representatives) receiving health care service at HIPAA covered programs must receive a HIPAA-compliant notice that describes:

- How the Agency uses and discloses PHI
- The clients' rights concerning their PHI
- How the client can make complaints (both to the Agency and to the Office of Civil Rights) concerning privacy or security issues

Prior to providing services, the Agency must make a good faith effort to obtain a written acknowledgment from the service recipient that he/she has received the Agency's Privacy Notice.

If the Agency is unable to obtain the acknowledgment, it must document the attempt that was made, and the reasons why such attempt was not successful. Further attempts to provide the notice and obtain acknowledgment must be made as soon as reasonably practicable after emergency treatment.

The Agency's notice covers the Agency and its non-employed clinical staff with regard to services rendered at the Agency. As such, all staff employed at HIPAA covered programs must be familiar with this document if they are involved with medical records.

Program Directors are responsible for reviewing registration procedures to ensure clients and residents, at all locations, are receiving a HIPAA-compliant Privacy Notice.

HIPAA JOINT PRIVACY NOTICE

THIS JOINT NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

INTRODUCTION

This Joint Notice is being provided to you on behalf of Catholic Charities of Long Island and the practitioners with clinical privileges that work at the Agency with respect to services provided at the Agency facilities (collectively referred to herein as "We" or "Our"). We understand that your medical information is private and confidential. Further, we are required by law to maintain the privacy of "protected health information." "Protected health information" or "PHI" includes any individually identifiable information that we obtain from you or others that relates to your past, present or future physical or mental health, the health care you have received, or payment for your health care. We will share protected health information with one another, as necessary, to carry out treatment, payment or health care operations relating to the services to be rendered at the Agency facilities.

As required by law, this notice provides you with information about your rights and our legal duties and privacy practices with respect to the privacy of PHI. This notice also discusses the uses and disclosures we will make of your PHI. We must comply with the provisions of this notice as currently in effect, although we reserve the right to change the terms of this notice from time to time and to make the revised notice effective for all PHI we maintain. You can always request a written copy of our most current privacy notice from the Site Coordinator at the Agency or you can access it on our website at http://www.catholiccharities.cc.

PERMITTED USES AND DISCLOSURES

We can use or disclose your PHI for purposes of *treatment, payment and health care operations*. For each of these categories of uses and disclosures, we have provided a description and an example below. However, not every particular use or disclosure in every category will be listed.

- *Treatment* means the provision, coordination or management of your health care, including consultations between health care providers relating to your care and referrals for health care from one health care provider to another. For example, a psychologist treating you may need to know from your psychiatrist if you are on any medications.

- *Payment* means the activities we undertake to obtain reimbursement for the health care provided to you, including billing, collections, claims management, determinations of eligibility and coverage and other utilization review activities. For example, we may need to provide PHI to your Third Party Payor to determine whether the proposed course of treatment will be covered or if necessary to obtain payment. Federal or state law may require us to obtain a written release from you prior to disclosing certain specially protected PHI for payment purposes, and we will ask you to sign a release when necessary under applicable law.

- *Health care operations* means the support functions of the Agency, related to *treatment* and *payment*, such as quality assurance activities, case management, receiving and responding to patient comments and complaints, physician reviews, compliance programs, audits, business planning, development, management and administrative activities. For example, we may use your PHI to evaluate the performance of our staff when caring for you. We may also combine PHI about many patients to decide what additional services we should offer, what services are not needed, and whether certain new treatments are effective. We may also disclose PHI for review and learning purposes. In addition, we may remove information that identifies you so that others can use the de-identified information to study health care and health care delivery without learning who you are.

OTHER USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

We may also use your PHI in the following ways:

- To provide appointment reminders for treatment or medical care.

- To tell you about or recommend possible treatment alternatives or other health-related benefits and services that may be of interest to you.

- To your family or friends or any other individual identified by you to the extent directly related to such person's involvement in your care or the payment for your care. We may use or disclose your PHI to notify, or assist in the notification of, a family member, a personal representative, or another person responsible for your care, of your location, general condition or death. If you are available, we will give you an opportunity to object to these disclosures, and we will not make these disclosures if you object. If you are not available, we will determine whether a disclosure to your family or friends is in your best interest, taking into account the circumstances and based upon our professional judgment.

- When permitted by law, we may coordinate our uses and disclosures of PHI with public or private entities authorized by law or by charter to assist in disaster relief efforts.

- We may contact you as part of our fundraising and marketing efforts as permitted by applicable law. You have the right to opt out of receiving such fundraising communications.

- We may use or disclose your PHI for research purposes, subject to the requirements of applicable law. For example, a research project may involve comparisons of the health and recovery of all patients who received a particular medication. All research projects are subject to a special approval process which balances research needs with a patient's need for privacy. When required, we will obtain a written authorization from you prior to using your health information for research.

- We will use or disclose PHI about you when required to do so by applicable law.

Note: Incidental uses and disclosures of PHI sometimes occur and are not considered to be a violation of your rights. Incidental uses and disclosures are by-products of otherwise permitted uses or disclosures which are limited in nature and cannot be reasonably prevented.

SPECIAL SITUATIONS

Subject to the requirements of applicable law, we will make the following uses and disclosures of your PHI:

- Organ and Tissue Donation. If you are an organ donor, we may release PHI to organizations that handle organ procurement or transplantation as necessary to facilitate organ or tissue donation and transplantation.

- Military and Veterans. If you are a member of the Armed Forces, we may release PHI about you as required by military command authorities. We may also release PHI about foreign military personnel to the appropriate foreign military authority.

- Worker's Compensation. We may release PHI about you for programs that provide benefits for work-related injuries or illnesses.

- Public Health Activities. We may disclose PHI about you for public health activities, including disclosures:

  * to prevent or control disease, injury or disability;
  * to report births and deaths;
  * to report child abuse or neglect;
  * to persons subject to the jurisdiction of the Food and Drug Administration (FDA) for activities related to the quality, safety, or effectiveness of FDA-regulated products or services and to report reactions to medications or problems with products;
  * to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
  * to notify the appropriate government authority if we believe that an adult patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if the patient agrees or when required or authorized by law.

- Health Oversight Activities. We may disclose PHI to federal or state agencies that oversee our activities (e.g., providing health care, seeking payment, and civil rights).

- Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose PHI subject to certain limitations.

- Law Enforcement. We may release PHI if asked to do so by a law enforcement official:

  * In response to a court order, warrant, summons or similar process;
  * To identify or locate a suspect, fugitive, material witness, or missing person;
  * About the victim of a crime under certain limited circumstances;
  * About a death we believe may be the result of criminal conduct;
  * About criminal conduct on our premises; or
  * In emergency circumstances, to report a crime, the location of the crime or the victims, or the identity, description or location of the person who committed the crime.

- Coroners, Medical Examiners and Funeral Directors. We may release PHI to a coroner or medical examiner. We may also release PHI about patients to funeral directors as necessary to carry out their duties.

- National Security and Intelligence Activities. We may release PHI about you to authorized federal officials for intelligence, counterintelligence, other national security activities authorized by law or to authorized federal officials so they may provide protection to the President or foreign heads of state.

- Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release PHI about you to the correctional institution or law enforcement official. This release would be necessary (1) to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

- Serious Threats. As permitted by applicable law and standards of ethical conduct, we may use and disclose PHI if we, in good faith, believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public or is necessary for law enforcement authorities to identify or apprehend an individual.

  ***Note*: HIV-related information, genetic information, alcohol and/or substance abuse records, mental health records and other specially protected health information may enjoy certain special confidentiality protections under applicable state and federal law. Any disclosures of these types of records will be subject to these special protections.**

OTHER USES OF YOUR HEALTH INFORMATION

Certain uses and disclosures of PHI will be made only with your written authorization, including uses and/or disclosures: (a) of psychotherapy notes (where appropriate); (b) for marketing purposes; and (c) that constitute a sale of PHI under the Privacy Rule. Other uses and disclosures of PHI not covered by this notice or the laws that apply to us will be made only with your written authorization. You have the right to revoke that authorization at any time, provided that the revocation is in writing, except to the extent that we already have taken action in reliance on your authorization.

YOUR RIGHTS

You have the right to request restrictions on our uses and disclosures of PHI for treatment, payment and health care operations. However, we are not required to agree to your request. We are, however, required to comply with your request if it relates to a disclosure to your health plan regarding health care items or services for which you have paid the bill in full. To request a restriction, you may make your request in writing to the Privacy Officer.

You have the right to reasonably request to receive confidential communications of your PHI by alternative means or at alternative locations. To make such a request, you may submit your request in writing to the Privacy Officer.

You have the right to inspect and copy the PHI contained in our Agency records, except:

- for psychotherapy notes, (i.e., notes that have been recorded by a mental health professional documenting counseling sessions and have

been separated from the rest of your medical record);

- for information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- for PHI involving laboratory tests when your access is restricted by law;
- if you are a prison inmate, and access would jeopardize your health, safety, security, custody, or rehabilitation or that of other inmates, any officer, employee, or other person at the correctional institution or person responsible for transporting you;
- if we obtained or created PHI as part of a research study, your access to the PHI may be restricted for as long as the research is in progress, provided that you agreed to the temporary denial of access when consenting to participate in the research;
- for PHI contained in records kept by a federal agency or contractor when your access is restricted by law; and
- for PHI obtained from someone other than us under a promise of confidentiality when the access requested would be reasonably likely to reveal the source of the information.
- for other reasons permitted by applicable State or Federal law.

In order to inspect or obtain a copy your PHI, you may submit your request in writing to the Site Coordinator. If you request a copy, we may charge you a fee for the costs of copying and mailing your records, as well as other costs associated with your request.

We may also deny a request for access to PHI under certain circumstances if there is a potential for harm to yourself or others. If we deny a request for access for this purpose, you have the right to have our denial reviewed in accordance with the requirements of applicable law.

You have the right to request an amendment to your PHI but we may deny your request for amendment, if we determine that the PHI or record that is the subject of the request:

was not created by us, unless you provide a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;

is not part of your medical or billing records or other records used to make decisions about you;

is not available for inspection as set forth above; or

is accurate and complete.

In any event, any agreed upon amendment will be included as an addition to, and not a replacement of, already existing records. In order to request an amendment to your PHI, you must submit your request in writing to Site Coordinator at our Agency, along with a description of the reason for your request.

You have the right to receive an accounting of disclosures of PHI made by us to individuals or entities other than to you for the six years prior to your request, except for disclosures:

- to carry out treatment, payment and health care operations as provided above;
- incidental to a use or disclosure otherwise permitted or required by applicable law;
- pursuant to your written authorization;
- for the Agency's directory or to persons involved in your care or for other notification purposes as provided by law;
- for national security or intelligence purposes as provided by law;
- to correctional institutions or law enforcement officials as provided by law;
- as part of a limited data set as provided by law.

To request an accounting of disclosures of your PHI, you must submit your request in writing to the Site Coordinator at our Agency. Your request must state a specific time period for the accounting (e.g., the past three months). The first accounting you request within a twelve (12) month period will be free. For additional accountings, we may charge you for the costs of providing the list. We will notify you of the costs involved, and you may choose to withdraw or modify your request at that time before any costs are incurred.

You have the right to receive a notification, in the event that there is a breach of your unsecured PHI, which requires notification under the Privacy Rule.

COMPLAINTS

If you believe that your privacy rights have been violated, you should immediately contact the Agency Privacy Officer by telephone at 516-733-7093 or by e-mail at Bruno.Julia@catholiccharities.cc. We will not take action against you for filing a complaint. You also may file a complaint with the Secretary of the U. S. Department of Health and Human Services.

CONTACT PERSON

If you have any questions or would like further information about this notice, please contact the Agency Privacy Officer by telephone at 516-733-7093 or by e-mail at Bruno.Julia@catholiccharities.cc.

This notice is effective as of September 23, 2013.

SAMPLE ACKNOWLEDGMENT

I, _____, acknowledge that I have been provided with a copy of Catholic Charities of Long Island's Privacy Notice.

Date:_____, 202___

Signature_____

AVISO DE PRIVACIDAD CONJUNTO HIPAA

ESTE AVISO CONJUNTO DESCRIBE CÓMO SE PUEDE USAR Y DIVULGAR SU INFORMACIÓN MÉDICA Y CÓMO PUEDE OBTENER ACCESO A ESTA INFORMACIÓN. POR FAVOR REVÍSELO CUIDADOSAMENTE.

INTRODUCCIÓN

Este aviso conjunto se le proporciona en nombre de **Catholic Charities de Long Island** y de los profesionales con privilegios clínicos que trabajan en la Agencia con respecto a los servicios proporcionados en las instalaciones de la Agencia (denominados en conjunto "Nosotros" o "Nuestro"). Comprendemos que su información médica es privada y confidencial. Además, la ley requiere que nosotros mantengamos la privacidad de la "información protegida de salud". La "información protegida de salud" o "PHI", por sus siglas en inglés, incluye cualquier información que se pueda identificar individualmente que nosotros obtengamos de usted o de otros y que se relacione con su salud física o mental pasada, presente o futura, el cuidado de la salud que ha recibido, o el pago por el cuidado de su salud. Compartiremos la información protegida de salud con otros según sea necesario, para llevar a cabo tratamiento, para el pago de operaciones de cuidado de la salud en relación con los servicios a ser prestados por las instalaciones de la Agencia.

Según lo requiere la ley, este aviso le proporciona información acerca de sus derechos y nuestros deberes legales y prácticas de privacidad con respecto a la privacidad de PHI. Este aviso también discute los usos y divulgaciones que haremos de su PHI. Debemos cumplir con las provisiones de este aviso según se encuentran vigentes actualmente, aunque nos reservamos el derecho de cambiar los términos de este aviso de tiempo en tiempo y hacer valer el aviso revisado para toda la PHI que mantengamos. Siempre puede solicitar una copia por escrito de nuestro aviso de privacidad más actual al Coordinador de Sitio en la Agencia o puede accederlo a través de nuestro sitio web en http://www.catholiccharities.cc.

USOS PERMITIDOS Y DIVULGACIONES

Podemos usar o divulgar su PHI con propósitos de tratamiento, pago y operaciones de cuidado de la salud.

Hemos proporcionado una descripción y un ejemplo debajo para cada una de estas categorías. Sin embargo, no se enlistará cada uso o divulgación particular en cada categoría.

- *Tratamiento* significa la provisión, coordinación o administración del cuidado de su salud, incluyendo las consultas entre proveedores de cuidado de la salud en relación con su cuidado y referencias para cuidado de la salud de un proveedor de cuidado de la salud a otro. Por ejemplo, un psicólogo que lo esté tratando puede necesitar saber de su psiquiatra si usted está tomando algún medicamento.
- *Pago* significa las actividades que emprendemos para obtener un reembolso por el cuidado de la salud que le proporcionamos, incluyendo la facturación, cobranza, gestión de reclamos, determinación de elegibilidad y cobertura y otras actividades de revisión de utilización. Por ejemplo, es posible que necesitemos proporcionar PHI a su parte pagadora para determinar si el curso de tratamiento propuesto estará cubierto o si es necesario obtener un pago. La ley federal o estatal nos puede requerir que obtengamos una liberación por escrito de su parte antes de divulgar cierta PHI especialmente protegida para propósitos de pago, y le pediremos que firme una liberación cuando sea necesario bajo la ley aplicable.
- *Operaciones* de cuidado de la salud significa las funciones de apoyo de la Agencia, en relación al tratamiento y pago, tal como actividades de aseguramiento de la calidad, gestión de caso, recibir y responder comentarios y quejas del paciente, revisiones médicas, programas de cumplimiento, auditorias, planeación de negocios, desarrollo, administración y actividades administrativas. Por ejemplo, podemos usar su PHI para evaluar el desempeño de nuestro personal al cuidarlo. También podemos combinar el PHI de muchos pacientes para decidir cuales servicios adicionales debemos ofrecer, cuales servicios no son necesarios y si ciertos tratamientos nuevos son efectivos. También podemos divulgar PHI para propósitos de revisión y aprendizaje. Además, podemos retirar la información que lo identifique para que otros puedan usar la información sin identificar para estudiar el cuidado de la salud y la prestación de cuidados de la salud sin saber quién es usted.

OTROS USOS Y DIVULGACIONES DE INFORMACIÓN PROTEGIDA DE SALUD

También podemos utilizar su PHI de las siguientes maneras:

- Para proporcionar recordatorios de citas para tratamiento o cuidado médico.

- Para informarle sobre o recomendarle alternativas posibles de tratamiento u otros beneficios y servicios relacionados con la salud que le puedan interesar.

- A su familia o amigos o cualquier otro individuo identificado por usted al grado en que dicha persona esté directamente relacionada con su cuidado o con el pago de su cuidado. Podemos usar o divulgar su PHI para notificar a, asistir en la notificación de, un miembro de la familia, un representante personal u otra persona responsable de su cuidado, sobre su ubicación, condición general o fallecimiento. Si usted está disponible, le daremos la oportunidad de objetar estas divulgaciones, y no las haremos si usted las objeta. Si usted no está disponible, nosotros determinaremos si la divulgación a su familia o amigos es en su mejor interés, tomando en cuenta las circunstancias y con base en nuestro juicio profesional.

- Cuando la ley lo permita, podemos coordinar nuestros usos y divulgaciones de PHI con las entidades públicas o privadas autorizadas por la ley o por estatuto para ayudar en esfuerzos de alivio de desastres.

- Lo podemos contactar como parte de nuestros esfuerzos de recaudación de fondos y mercadeo según lo permite la ley aplicable. Tiene el derecho de elegir no recibir dichas comunicaciones sobre recaudación de fondos.

- Podemos usar o divulgar su PHI con propósitos de investigación, sujeto a los requisitos de ley aplicables. Por ejemplo, un proyecto de investigación puede involucrar la comparación de la salud y recuperación de todos los pacientes que recibieron un medicamento en particular. Todos los proyectos de investigación están sujetos a un proceso especial de aprobación que equilibra las necesidades de la investigación con la necesidad de privacidad del paciente. Cuando se requiera, obtendremos una autorización por escrito de su parte antes de usar su información de salud para investigación.

- Usaremos o divulgaremos PHI sobre usted cuando nos lo requiera la ley aplicable.

Nota: Algunas veces ocurren usos y divulgaciones incidentales de PHI y no se consideran como una violación de sus derechos. Los usos y divulgaciones incidentales son subproductos de los usos o divulgaciones permitidos que son de naturaleza limitada y que no pueden prevenirse razonablemente.

SITUACIONES ESPECIALES

Sujeto a los requerimientos de la ley aplicable, haremos los siguientes usos y divulgaciones de su PHI:

- Donación de órganos y tejidos. Si usted es un donante de órganos, podemos divulgar su PHI a organizaciones que se encargan de la obtención de órganos o de trasplantes según sea necesario para facilitar la donación de órganos o tejidos y los trasplantes.

- Militares y Veteranos. Si usted es un miembro de las Fuerzas Armadas podemos divulgar PHI sobre usted según lo requieran las autoridades de comando militar. También podemos divulgar PHI sobre personal militar extranjero a la autoridad militar extranjera adecuada.

- Compensación de los trabajadores. Podemos divulgar PHI sobre usted para programas que proporcionen beneficios por lesiones o enfermedades relacionados con el trabajo.

- Actividades de salud pública. Podemos divulgar PHI sobre usted para actividades de salud pública, incluyendo divulgaciones:

    - Para prevenir o controlar enfermedades, lesiones o discapacidad;
    - Para reportar nacimientos o muertes;
    - Para reportar abuso infantil o negligencia;
    - A las personas sujetas a la jurisdicción de la Administración de Alimentos y Medicamentos (FDA, por sus siglas en inglés) para actividades relacionadas con la calidad, seguridad o efectividad de productos o servicios regulados por la FDA y para reportar reacciones a medicamentos o problemas con productos;
    - Para notificar a alguna persona que haya estado expuesta a una enfermedad o que pueda estar en riesgo de contraer o diseminar una enfermedad o condición;
    - Para notificar a la autoridad apropiada en el gobierno si creemos que un paciente adulto ha sido víctima de abuso, negligencia o violencia doméstica. Solo haremos esta divulgación si el paciente lo acuerda o cuando la ley lo requiera o autorice.

- Actividades de supervisión de la salud. Podemos divulgar su PHI a agencias federales o estatales que supervisan nuestras actividades (ejemplo, proporcionar cuidado de la salud, obtención de pagos y derechos civiles).

- Demandas y disputas. Si usted está involucrado en una demanda o disputa, podemos divulgar PHI sujeto a ciertas limitaciones.

- Aplicación de la Ley. Podemos divulgar PHI si nos lo pide un oficial de aplicación de la ley:

    - En respuesta a una orden de la corte, orden judicial, citación o proceso similar;
    - Para identificar o ubicar a un sospechoso, fugitivo, testigo material o persona extraviada;
    - Sobre la victima de un crimen bajo ciertas circunstancias limitadas;
    - Sobre un fallecimiento que creamos que pudo haber sido el resultado de una conducta criminal;
    - Sobre conducta criminal en nuestras instalaciones; o
    - En circunstancias de emergencia, para reportar un crimen, la ubicación del crimen o de las víctimas, o la identidad, descripción o ubicación de las personas que cometieron el crimen.

- Forenses, examinadores médicos y directores de funerarias. Podemos divulgar PHI a un forense o examinador médico. También podemos divulgar PHI sobre pacientes a los directores de las funerarias según sea necesario para que lleven a cabo sus deberes.

- Actividades de seguridad nacional e inteligencia. Podemos divulgar PHI sobre usted a los oficiales federales autorizados para inteligencia, contrainteligencia, otras actividades de seguridad nacional autorizadas por la ley o a oficiales federales autorizados para que estos puedan

proporcionar protección al presidente o a jefes de estado extranjeros.

- Presos. Si usted está preso en una institución correccional o bajo la custodia de un oficial de aplicación de la ley, podemos divulgar PHI sobre usted a la institución correccional u oficial de aplicación de la ley. Esta divulgación sería necesaria (1) para proporcionarle cuidados de la salud; (2) para proteger su salud y seguridad o la salud y seguridad de otros; o (3) para la seguridad de la institución correccional.

- Amenazas graves. Según lo permita la ley aplicable y los estándares de conducta ética, podemos usar y divulgar PHI si, de buena fe, creemos que su uso o divulgación es necesario para prevenir o disminuir una amenaza seria e inminente a la salud o seguridad de una persona o del público o si es necesario para las autoridades de aplicación de la ley para identificar o aprehender a un individuo.

Nota: La información relacionada con el VIH, información genética, registros de abuso de alcohol y/o sustancias, registros de salud mental y otra información de salud especialmente protegida pueden gozar de ciertas protecciones especiales de confidencialidad bajo las leyes estatales y federales aplicables. Cualquier divulgación de este tipo de registros estará sujeta a esas protecciones especiales.

OTROS USOS DE SU INFORMACIÓN DE SALUD

Solo se harán ciertos usos o divulgaciones de PHI con su autorización por escrito, incluyendo los usos y/o divulgaciones: (a) de notas de psicoterapia (cuando sea apropiado); (b) para propósitos de mercadeo; y (c) que constituyan una venta de PHI bajo la Ley de Privacidad. Otros usos y divulgaciones de PHI que no estén cubiertos en este aviso o por las leyes que se apliquen a nosotros solo se harán por medio de su autorización por escrito. Usted tiene el derecho de revocar esa autorización en cualquier momento, previsto que la revocación sea por escrito, excepto al grado en que ya hayamos tomado acción bajo su autorización.

SUS DERECHOS

1. Tiene derecho a solicitar una restricción para nuestros usos y divulgaciones de PHI para tratamiento, pago y operaciones de cuidado de la salud. Sin embargo, no estamos obligados a respetar su solicitud. Sin embargo, estamos obligados a cumplir con su solicitud si se relaciona con una divulgación de su plan de salud con respecto a artículos de cuidado de la salud o servicios para los cuales usted haya pagado el total de la factura. Para solicitar una restricción, puede presentarle su solicitud por escrito al Oficial de Privacidad.

2. Tiene derecho a solicitar recibir comunicaciones confidenciales de su PHI por medios alternos o en ubicaciones alternas según sea razonable. Para hacer tal solicitud, puede enviar su solicitud por escrito al Oficial de Privacidad.

3. Tiene derecho a inspeccionar y copiar la PHI contenida en los registros de nuestra Agencia, excepto:

(i) Para notas de psicoterapia, (ejemplo, notas que hayan sido registradas por un profesional de salud mental que haya estado documentando sesiones de asesoría y que haya sido separado del resto de su expediente médico);

(ii) Para información compilada con anticipación razonable a, o para uso en, una acción o procedimiento civil, criminal o administrativo;

(iii) Para PHI que involucre pruebas de laboratorio cuando su acceso esté restringido por la ley;

(iv) Si usted es un interno en la prisión, y el acceso podría poner en peligro su salud, seguridad, custodia o rehabilitación o la de otros internos, cualquier oficial, empleado o cualquier otra persona en la institución correccional o persona responsable de transportarlo;

(v) Si obtuvimos o creamos PHI como parte de un estudio de investigación, su acceso al PHI puede estar restringido mientras la investigación esté en curso, previsto que usted acordó la negación temporal de acceso al consentir participar en la investigación;

(vi) Para PHI contenida en los registros mantenidos por una agencia federal o contratista cuando su acceso sea restringido por la ley; y

(vii) Para PHI obtenido de alguien que no seamos nosotros bajo promesa de confidencialidad cuando sea razonablemente probable que el acceso solicitado revele la fuente de la información.

(viii) Por otras razones permitidas por la ley federal o estatal aplicable.

Para inspeccionar u obtener una copia de su PHI, puede enviar su solicitud por escrito al Coordinador de Sitio. Si solicita una copia, podemos cobrarle una cuota por los costos de copiar y enviar sus registros por correo, así como cualquier otro costo asociado con su solicitud.

También podemos negar una solicitud de acceso a PHI bajo ciertas circunstancias si hay potencial de daños a usted mismo o a otros. Si negamos una solicitud de acceso para este propósito, usted tiene el derecho de que se revise la negativa de conformidad con los requisitos de la ley aplicable.

4. Tiene el derecho de solicitar una enmienda de su PHI pero nosotros podemos negar su solicitud de enmienda, si determinamos que el PHI o registro objeto de la solicitud:

(i) No fue creado por nosotros, a menos de que usted proporcione una base razonable para creer que el autor del PHI ya no está disponible para actuar de conformidad con la enmienda solicitada;

(ii) No sea parte de sus registros médicos o de facturación u otros registros usados para tomar decisiones sobre usted;

(iii) No está disponible para inspección según lo establecido arriba; o

(iv) Está correcto y completo.

En cualquier caso, cualquier enmienda acordada será incluida como una adición a, no como un reemplazo de, un registro ya existente. Para solicitar una enmienda a su PHI, debe enviar su solicitud por escrito al Coordinador de Sitio en nuestra Agencia, junto con una descripción de la razón de su solicitud.

5. Tiene el derecho de recibir un informe de las divulgaciones de PHI hechas por nosotros a individuos o entidades que no sean usted para los seis años previos a su solicitud, excepto por divulgaciones:

(i) llevar a cabo tratamiento, pago y operaciones de cuidado de la salud según lo previsto arriba;

(ii) Incidentales a un uso o divulgación permitida o requerida de cualquier otra manera por la ley aplicable;

(iii) De conformidad con su autorización por escrito;

(iv) Para el directorio de la Agencia o las personas involucradas en su cuidado o para otros propósitos de notificación según lo previsto por la ley;

(v) Para propósitos de seguridad nacional o inteligencia según lo previsto por la ley;

(vi) Para instituciones correccionales u oficiales de aplicación de la ley según lo previsto por la ley;

(vii) Como parte de un conjunto limitado de datos según lo previsto por la ley.

Para solicitar un informe de las divulgaciones de su PHI, usted debe enviar su solicitud por escrito al Coordinador de Sitio en nuestra agencia. Su solicitud debe tener un periodo específico de tiempo para el informe (ejemplo, de los últimos tres meses). El primer informe que usted solicite dentro de un periodo de doce (12) meses será gratuito. Para informes adicionales, le podríamos cobrar el costo de proporcionarle la lista. Le notificaremos los costos involucrados, y usted puede elegir retirar o modificar su solicitud en ese momento antes de incurrir en algún costo.

6. Tiene derecho a recibir una notificación, en caso de que haya algún incumplimiento con respecto a su PHI no asegurado, que requiera una notificación bajo la Ley de Privacidad.

QUEJAS

Si usted cree que sus derechos de privacidad han sido violados, debe contactar inmediatamente al Oficial de Privacidad de la Agencia por teléfono al **516-733-7093 o por correo electrónico a Bruno.Julia@catholiccharities.cc**. No tomaremos ninguna acción contra usted por presentar una queja. También puede presentar su queja en la Secretaría del Departamento de Salud y Servicios Humanos de los EE.UU.

PERSONA DE CONTACTO

Si tiene alguna pregunta o quisiera más información sobre este aviso, por favor contacte al Oficial de Privacidad de la Agencia al teléfono **516-733-7093 o por correo electrónico a Bruno.Julia@catholiccharities.cc**

Este aviso tendrá validez a partir del 23 de septiembre de 2013.

ACUSE DE RECIBO MUESTRA

Yo, _____, reconozco que se me ha proporcionado una copia del Aviso de Privacidad de Catholic Charities de Long Island.

Fecha: _____, 202____.

Firma _____

HIPAA PRIVACY TOOL #5

DEFINITIONS AND EXAMPLES OF TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

Definitions	Examples
Treatment means the provision, coordination, and/or management of health care and related services by one or more health care providers, including: (i) the coordination or management of health care by a health care provider with a third party; (ii) (ii) a consultation between health care providers relating to a client; or (iii) (iii) the referral of a client for health care.	**Example 1:** A client receives care at the Agency, and the Agency refers the client to a hospital for inpatient treatment. **Example 2:** A therapist consults with a medical doctor regarding a client and makes a referral.
Payment (for health care providers) means the activities undertaken by a health care provider to obtain reimbursement for the provision of health care, including: (i) determinations of eligibility or coverage; (ii) (ii) billing, claims management, collection activities and related data processing; (iii) (iii) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (iv) utilization review activities (including pre-certification and pre-authorization of services); and (v) disclosures to consumer reporting agencies for collection purposes of any of the following information of a client: name, address, date of birth, social security number, payment history, or account number.	**Example 1:** The Agency's intake coordinator checks to see if a client is currently covered by Oxford. **Example 2:** The Agency's client accounts department bills the client or the client's health insurance for health care. **Example 3:** The Agency files a credit report regarding a client that does not pay fees owed to the Agency.
Health Care Operations (for health care providers only) includes any of the following activities: (i) Conducting quality assessment and improvement activities, including outcomes evaluations, the development of clinical guidelines for the provider, protocol development, population-based activities relating to improving health or reducing health care costs, case management and care coordination, contacting providers and clients regarding treatment alternatives, and related functions; (ii) Reviewing the competence or qualifications of health care professionals, evaluating practitioner performance, training health care professionals and non-health care professionals, and accreditation, certification, licensing, and credentialing activities;	**Example 1:** The Agency engages in performance improvement activities and develops specific clinical guidelines. **Example 2:** The Agency reviews the qualifications, competency and credentials of a therapist seeking employment.

(iii) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;	**Example 3:** The Agency conducts a fraud and abuse compliance program which, among other things, reviews health care claims.
(iv) Business planning and development, such as conducting cost-management and planning-related analysis related to managing and operating a professional practice or health care facility; and	**Example 4:** The Agency reviews its books in order to develop a budget and improve its profitability.
(v) Business management and general administrative activities of the practice, including: implementation of and compliance with HIPAA; customer service; resolution of internal grievances; the sale, transfer, merger or consolidation of all or part of the Covered Entity with another Covered Entity (or an entity that following such activity, will become a Covered Entity) and due diligence related to such activity; creating de-identified PHI or a limited data set; and fund raising for the benefit of the Covered Entity.	**Example 5:** The Agency discloses its books and client account information to another mental health facility during the merger of the two facilities.

PRIVACY TOOL # 6

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **DISCLOSURES TO FAMILY MEMBERS, FRIENDS AND PERSONAL REPRESENTATIVES**

REFERENCES: **45 CFR §§ 164.502(g)**

EFFECTIVE DATE: **September 22, 2013**

APPROVED BY:

I. GENERAL POLICY

Subject to the rules discussed below, the Agency may disclose a Client's health information to family members and friends involved in the Client's health care or payment for health care.

Note: To the extent that Client information includes HIV-related information, genetic information, alcohol and/or substance abuse treatment records, or mental health treatment records, special confidentiality protections under Federal and/or State law must be considered. Questions regarding the disclosure of these types of information or records should be raised with the Agency's Privacy Officer or with counsel.

II. DISCLOSURES TO FAMILY MEMBERS[1] AND FRIENDS

A. Client Care and Payment. Unless stated otherwise below, the Agency's staff may disclose a Client's health information to a family member or friend of the Client or to any other person identified by the Client as being involved in the Client's care or payment for health care. The Agency's staff may continue to disclose such information after the Client's death, unless such disclosure is inconsistent with any prior expressed preferences of the decedent. Disclosures to family members, friends and other persons shall be limited to the health information that is directly relevant to their involvement with the Client's health care or payment for health care.

[1] A family member of a patient is defined as (1) any individual who is or may become eligible for coverage under the terms of a group health plan because of the individual's relationship to the patient (a "Dependent"), or (2) any person who is a parent, spouse, sibling, child, grandparent, grandchild, aunt, uncle, nephew, niece, great-grandparent, great-grandchild, great aunt, great uncle, first cousin, great-great-grandparent, great-great-grandchild, or child of a first cousin of the patient or of the Dependent.

1. Uses and Disclosures in the Presence of the Client. If a Client is available prior to disclosures to family members friends or personal representatives and has the capacity to make health care decisions, the use and disclose may be made only if the Agency's staff:

    a) *obtain the Client's agreement;*

    b) *provide the Client with the opportunity to object to the disclosure, and the Client does not express an objection; or*

    c) *reasonably infer from the circumstances, based on the exercise of professional judgment, that the Client does not object to the disclosure.*

2. Uses and Disclosures When the Client Is Incapacitated or Not Present. If the Client is not present, or if the Client cannot be given an opportunity to agree or object to a disclosure because of incapacity or an emergency, the Agency's staff may, in the exercise of professional judgment, disclose information that is directly relevant to the Client's care, to a family member, friend or another person otherwise identified by the Client. The Agency may also use professional judgment to make reasonable inferences regarding the Client's best interests when allowing a person to act on behalf of the Client to pick-up filled prescriptions, medical supplies, X-rays, or other similar forms of Client information.

B. Notification. The Agency's staff may use or disclose Client information to family members, personal representatives and others involved in the Client's care in order to notify, or assist in the notification of (including identifying or locating) the Client's location, general condition or death.

III. PERSONAL REPRESENTATIVES

A. Rights of Personal Representatives. The Agency is required by HIPAA's privacy regulations to treat a Client's personal representative as if he/she were the Client for purposes of making uses and disclosures of Client information to the personal representative and allowing the personal representative to exercise the Client's available privacy rights (including the right to access and request amendments to Client information).

B. Identification of Personal Representatives.

1. Adults and Emancipated Minors. If, under applicable law, a person has the authority to act on behalf of an adult or emancipated minor Client in making health care decisions, the Agency will treat such person as a personal representative of the Client. In New York, persons who have the authority to make health care decisions for another are "legal representatives." Examples of legal representatives include: health care agents, surrogates, and guardians legally appointed pursuant to applicable legal proceedings.[2]

[2] Under New York law, a guardian can be appointed for an adult pursuant to Article 81 of the Mental Hygiene Law and Article 17-A of the Surrogate's Court Procedure Act.

In addition, for deceased Clients, if an executor, administrator, or other person has authority under applicable law to act on behalf of the Client or the Client's estate, the Agency will treat such person as the Client's personal representative.

2. Unemancipated Minors. If under New York law, a parent, guardian[3] or other person acting *in loco parentis* for an unemancipated minor has the authority to act on behalf of the minor Client in making health care decisions, the Agency will treat such person as a personal representative with respect to the Client information relevant to such person's authority.

C. Limitations.

1. Even though a person may otherwise be considered a personal representative of a Client, the Agency may elect not to treat such person as the personal representative if the Agency has a reasonable belief that:

   a) The Client has been or may be subjected to domestic violence, abuse, or neglect by such person; or

   b) Treating such person as the personal representative could endanger the Client; and the Agency, in the exercise of professional judgment, decides that it is not in the best interest of the Client to treat the person as the Client's personal representative.

2. A parent, guardian or other person acting in loco parentis for an unemancipated minor may not be treated as a personal representative with respect to the minor's health information in the following situations:

   a) The minor consents to a health care service, no other consent to such health care service is required by law (regardless of whether the consent of another person has also been obtained), and the minor has not requested that such person be treated as a personal representative;

   b) The minor may lawfully obtain a health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

   c) A parent, guardian or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to a health care service.

[3] In this context, "guardian" refers to a guardian appointed pursuant to Article 17 of the Surrogate's Court Procedure Act, Article 81 of the Mental Hygiene Law, or other legally appointed guardians of minor patients who may be entitled to request access to a patient record.

Notwithstanding the foregoing, the Agency must comply with state law in allowing access to Client information in regard to an unemancipated minor.

Finally, when a parent, guardian or other person acting *in loco parentis* is not a personal representative (as defined in paragraph B, above) and no applicable provision under New York State or other law (including case law) grants access to the health information of an unemancipated minor, a Covered Entity may provide or deny access to such individual if the decision is consistent with New York State or other applicable law, provided that the decision is made by a licensed health care professional exercising professional judgment.

IV. VERIFICATION

Except with respect to disclosures to family members and friends, the Agency is required to verify the identity and authority of persons to whom Client information is disclosed, if the identity and authority are not known to the Agency. With regard to persons claiming to be personal representatives, the Agency will request verification of the identity of such persons by checking their driver's license, passport, or other identifying documentation. As proof of authority to make health care decisions on behalf of the Client, the Agency will review a copy of the applicable court order, health care proxy, or other legal documentation. The Agency may reasonably rely on such documents and representations as providing the required verification.

* * * * *

Any questions regarding disclosures to family members, friends or personal representatives or the verification of personal representatives should be raised with the Agency's Privacy Officer or with counsel.

PRIVACY TOOL #7

CATHOLIC CHARITIES

(the "Agency")

POLICY & PROCEDURE

SUBJECT: **USES AND DISCLOSURES OF CLIENT INFORMATION**

REFERENCES: **45 CFR §§ 160.103, 164.508, 164.510, 164.512, AND 164.522(a)**

EFFECTIVE DATE: September 22, 2013

APPROVED BY:

I. INTRODUCTION

This Policy and Procedure establishes the general rules which the Agency will follow when using and disclosing the health information of its Clients.

II. GENERAL RULES

A. Protected Health Information. HIPAA requires the Agency to adhere to certain rules when using and disclosing "protected health information" or "PHI" of its Clients. "Protected health information" is defined by HIPAA as information, in any form or medium (including oral, written and electronic communications), that is created by the Agency, relates to an individual's physical or mental health (e.g., provision of payment for) and identifies, or could be reasonably expected to be used to identify, an individual. Once a Client has been deceased for more than 50 years, such information about him or her is no longer considered to be PHI.

Protected Health Information includes everything from a Client's name, address and telephone number to the Client's clinical and billing records.

B. Use and Disclosure for Treatment, Payment and Health Care Operations. Consistent with the Agency's privacy notice to Clients, the Agency may use and disclose PHI of its Clients for the Agency's treatment, payment and health care operations purposes. No written consent or authorization is required for uses and disclosures of PHI for these purposes unless the Agency receives direct or indirect remuneration in exchange for the PHI.

C. Other Uses and Disclosures of PHI. The Agency will not use or disclose PHI for purposes other than treatment, payment and health care operations, except that the Agency may disclose PHI (as long as such disclosure is also permissible under NY State law):

1. to the Client.

2. for treatment activities of another health care provider (e.g., the Agency can provide PHI to a physician in order to assist the physician in treating a Client).

3. to another Covered Entity for its payment activities (e.g., to an ambulance company so that the ambulance company can submit an insurance claim for services it provided).

4. to another Covered Entity for certain of its health care operations,[4] provided the Agency and the Covered Entity each has or had a relationship with the Client and the PHI pertains to that relationship. *Note*: If the Agency participates in an organized health care arrangement ("OHCA"),[5] the Agency may disclose PHI to another Covered Entity that participates in the arrangement for any health care operations of the arrangement.

5. pursuant to a valid HIPAA authorization.

6. to a business associate,[6] subject to the terms of the applicable business associate agreement.

7. to the U.S. Department of Health and Human Services in connection with compliance reviews and investigations, subject to the requirements of applicable law.

8. to a Client's family, friends and personal representatives as described in the Agency policy regarding such disclosures.

9. to a person subject to the jurisdiction of the FDA for purposes related to a product approved by the FDA (e.g., incident reporting, tracking of products, product recalls or post-marketing surveillance).

10. for various legal, regulatory and employment purposes pursuant to the Agency's policy regarding such.

11. to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, subject to the requirements of HIPAA and applicable law.

12. in a limited data set that meets the requirement of HIPAA's privacy regulations, if the Agency enters into a data use agreement with the limited data set recipient.

13. limited to proof of immunization, to a Client's school if a) the school is required by state or other law to have such proof of immunization before admitting the individual; and b) the Agency has written or oral agreement from the Client or his or her personal representative, as applicable.

14. as otherwise specifically permitted or required by federal regulations.

---

[4] The purpose of such disclosure must be for quality assurance activities, process improvement, case management, population-based activities relating to improving health or reducing health care costs, protocol development, contacts with health care providers and Clients about treatment alternatives and related activities, training programs, accreditation, licensure, credentialing, or fraud and abuse compliance.

[5] An OHCA is an organized system of health care or a clinically integrated health care setting in which two or more providers participate (e.g., an admitting relationship between the Agency and its medical staff).

[6] Business Associate means a person/entity to whom the Agency provides Client information and who performs a task or function on behalf of the Agency.

Note: HIV, alcohol and/or substance abuse and mental health treatment records and genetic information enjoy additional confidentiality protections by state and federal law that must be followed. Questions concerning the disclosure of these types of information should be raised with the Privacy Officer.

D. Incidental Disclosures. Incidental uses or disclosures of PHI which occur as a by-product of an otherwise permitted or required use or disclosure are not considered to be violations of HIPAA, provided adequate safeguards have been put into place and minimum necessary policies have been implemented.

E. Agency's Privacy Notice. The Agency will provide Clients with a copy of a privacy notice which describes the Agency's uses and disclosures of PHI, the Client's privacy rights and the procedure for making complaints. In addition, the Agency will make a good faith effort to obtain each Client's written acknowledgment of receipt of the privacy notice. If the Agency is unable to do so, it will document the attempts that were made and why such attempts were unsuccessful.

F. Client Restrictions. The Client has the right to request restrictions on how the Agency uses or discloses their PHI to carry out treatment, payment and health care operations.

1. The Agency has to agree to restrictions made by Clients to restrict disclosure of PHI to a health plan if: a) the PHI pertains solely to health care items or services for which the Client has paid the Agency in full; and b) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law.

2. For all other Client restriction requests the Agency does not have to agree to such restrictions. When a request for a restriction is made by a Client, the Agency will inform the Client of the Agency's decision regarding a request for a restriction and will document that the request was made as well as the decision made by the Agency. ***RESTRICTIONS ARE DOCUMENTED AND MAINTAINED IN CLIENT'S CHART. STAFF MUST REVIEW FILE FOR RESTRICTIONS PRIOR TO MAKING A DISCLOSURE.***

3. Agency staff may not agree to any restrictions on the Agency's uses or disclosures of PHI without the prior approval of the Agency's Privacy Officer.

4. If the Agency agrees to a restriction requested by a Client, the Agency will honor the restriction, unless the Client subsequently agrees to terminate the restriction,[7] and except when otherwise required to provide emergency treatment to the Client.

G. Remuneration for PHI.

1. Except as listed below, if the Agency receives remuneration for PHI, the Agency may not disclose PHI for any purpose unless it has obtained the Client's authorization. The Agency may disclose PHI for the following purposes even if it is receiving direct or indirect remuneration in exchange for disclosing PHI:

[7] Either in writing or orally. Oral agreements to terminate a restriction should be documented by the Agency.

a) Public health activities;

b) Research purposes as long as the remuneration received is reasonable cost-based fee to cover the cost to prepare and transmit the information for research purposes;

c) Treatment and payment purposes;

d) Sale, transfer, merger, or consolidation of all or any part of the Agency and for related due diligence;

e) Services rendered by a business associate at the specific request of the Agency;

f) To a Client or their personal representative when requested; or

g) Otherwise required by law permitted under the privacy regulations.

III. CLIENT AUTHORIZATIONS

A. Authorization Required. If the Agency intends to use or disclose PHI for purposes other than treatment, payment or health care operations, and when the use or disclosure is not otherwise authorized under HIPAA, the Agency will first obtain a valid written and signed authorization from the Client or his or her personal representative. When the Agency receives a valid Client authorization, all uses and disclosures pursuant to the authorization must be consistent with its terms.

B. Who Can Execute an Authorization. The following individuals are authorized to sign an authorization:

1. The Client, provided that he/she is competent and at least 18 years old;

2. A personal representative with the legal authority to make medical decisions for an incapacitated Client, such as a court appointed guardian authorized to make medical decisions, health care agent, surrogate, parent, or other person acting *in loco parentis* that has the legal authority to make medical decisions on behalf of a minor subject to the Agency's policy and procedure regarding personal representatives;

3. A person, executor or administrator of a deceased Client who has the authority to act on behalf of a deceased Client or the Client's estate.

C. Documentation. The Agency will retain a written, signed copy of such authorization. This documentation will be retained for six (6) years from the date of the authorization's execution or the date when the authorization was last in effect, whichever is later.

D. Defective Authorizations. The Agency will not accept an authorization if:

1. the authorization's expiration date has passed or the expiration event is known by the Agency to have occurred;

2. the authorization that has not been filled out completely or contains material information known by the Agency to be false;

3. the authorization is known by the Agency to have been revoked or incorrectly created as a compound authorization.

E. Compound and Conditional Authorizations.

1. Except as indicated in this Section, the Agency will not condition a Client's treatment or payment on the Client's providing an authorization.

    a) The Agency may require the authorization if the purpose of providing the health care is to disclose the PHI to a third party. For example, if an Agency has a contract with an employer to provide fitness-for-duty exams to its employees, an Agency can refuse to conduct the exam if the employee refuses to provide an authorization to disclose the exam results to the employer.

    b) The Agency may also condition the provision of research-related treatment on the provision of an authorization.

2. Generally, an authorization for the use or disclosure of PHI will not be combined with any other document. Any type of authorization may, however, be combined with any other type of authorization, with the following exceptions and conditions:

    a) An authorization for a use or disclosure of psychotherapy notes can only be combined with another psychotherapy note authorization.

    b) An authorization for a research study may be combined with any other type of written permission for the same or another research study, including a consent to participate in such research.

    c) An authorization for a research study that conditions the provision of research-related treatment on the provision of the authorization may be combined with an authorization for other research activities that are not conditioned upon the provision of the authorization, if the compound authorization clearly differentiates between the conditioned and unconditioned research components and provides the individual with an opportunity to separately opt into (or not opt into) the research activities that are not conditioned upon authorization. For additional information regarding the use of research authorizations refer to the Agency's research policy.

    d) Except for authorizations regarding conditioned research related treatment and unconditioned research, authorizations that condition the provision of treatment or payment cannot be combined with other authorizations.

F. Revocations. An individual can revoke his or her authorization, in writing, at any time, except to the extent that the Agency has relied upon the authorization.

G. SPECIFIC AUTHORIZATIONS.

1. Authorizations for Psychotherapy Notes. There are special rules regarding release of psychotherapy notes. Generally, the Agency will obtain an authorization prior to using or disclosing a Client's psychotherapy notes for any purpose, except those listed below. Psychotherapy notes are the notes of a mental health professional that document or analyze conversations during a counseling session and are separated from the rest of the Client's medical record. Psychotherapy notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date.

An authorization will not be required; however, when the psychotherapy notes will be used or disclosed for the following purposes:

a) Use by the originator of the psychotherapy notes for treatment;

b) Use or disclosure by the Agency for its own mental health training programs;

c) Use and disclosure by the Agency to defend itself in a legal action or other proceeding brought by the Client;

d) Disclosures to DHHS to investigate the Agency's compliance with the law;

e) Uses and disclosures required the law, if the use or disclosure complies with and is limited to the relevant requirements of such law;

f) Disclosures to a health oversight agency in connection with the oversight of the originator of the psychotherapy notes;

g) Disclosures to coroners or medical examiners for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law; or

h) Consistent with applicable law and standards of ethical conduct, uses and disclosures which are based on a good faith belief of the Agency that such uses or disclosures are necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and such uses or disclosures are to a person or persons who may reasonably be able to prevent or lessen the threat.

2. Authorizations for Marketing. Generally, the Agency will not use or disclose PHI for marketing purposes unless it obtains a Client authorization. There are, however, several exceptions to the authorization requirement for marketing. Additionally, if marketing involves financial remuneration to the Agency from a third party, the authorization form must state that such remuneration is involved. For questions regarding marketing authorizations, refer to Agency's Marketing Policy.

3. Authorizations for Fundraising. The Agency may use Client demographic information, dates of health care service, department of service information, treating physician, outcome information, and health insurance status of the Client for fundraising purposes, so long as this use of the information is described in the notice to Clients. If the information is to be given to anyone other than a business associate or institutionally related foundation, a Client authorization is required. For questions regarding Fundraising authorizations, refer to the Agency's Fundraising Policy.

HIPAA PRIVACY TOOL #8

CATHOLIC CHARITIES

(the "Agency")

POLICY AND PROCEDURE

SUBJECT: **DE-IDENTIFYING AND RE-IDENTIFYING CLIENT'S HEALTH INFORMATION AND CREATION OF LIMITED DATA SETS**

REFERENCES: **45 CFR § 164.502(d); 45 CFR § 164.514(a)-(c) & (e)**

EFFECTIVE DATE: **April 1, 2003**

APPROVED BY:

1. Purpose

The Agency is required by law to maintain the confidentiality and privacy of a client's identifiable health information. This policy and procedure explains how the Agency determines whether a client's health information is (i) identifiable and requested to be protected or (ii) is sufficiently de-identified so that it is not subject to the confidentiality and private rules. This policy also explains under what circumstances de-identified health information may be re-identified by the Agency. Finally, this policy and procedure explains (i) the method by which a limited data set of client health information can be created and (ii) the circumstances under which limited data sets can be used and disclosed for research, public health and health care operations purposes.

2. De-Identified Health Information

A. All client identifiable health information which has been "de-identified" (as described below) can be used or disclosed without complying with HIPAA. Health information is considered de-identified information if it does not directly or indirectly identifies a client. For information to be considered de-identified (i.e., does not identify a client or cannot be used to identify a client) it must satisfy all of the requirements of either B(i) or B(ii), below).

B. Any individual or program wishing to create or utilize de-identified information should contact the **Privacy Officer**, who will ensure one of the two following HIPAA-compliant de-identification methodologies is properly followed.

i. A person or entity with appropriate knowledge of generally accepted statistical and scientific principles and methods for rendering information anonymous is engaged to determine that (a) the risk is very small that the information could be used (alone or in

combination with other reasonably available information) by an anticipated recipient to identify an individual, and (b) documents the basis for such determination. The Agency recommends that the **Entity to Be Used for De-identification recommended by the Privacy Officer** be utilized for all such purposes, although a different person or entity may be engaged provided approval of the **Privacy Officer** is obtained.

ii. All of the following identifiers of the individual and relatives, employers, or household members of the individual, have been properly removed from the information:

a. Names;

b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, (except for the initial three digits of a zip code if the geographic unit formed by such three digits contains more than 20,000 people);

c. *Except for calendar years*, all dates related to an individual such as birth date, admission date, discharge date, date of death; provided however, that all individuals over 89 years of age may only be aggregated into a single category of age 90 or older and may not be categorized by calendar year;

d. Telephone numbers;

e. Fax numbers;

f. Electronic mail addresses;

g. Social security numbers;

h. Medical record numbers;

i. Health plan beneficiary numbers;

j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; and

r. Any other unique identifying number, characteristic, or code (excluding the re-identification code described in III below).

The Agency requires that any information de-identified in this manner be approved by the **Privacy Officer** prior to use or disclosure.

3. Re-Identifying De-Identified Health Information

A. The Agency may, at its discretion, decode or translate de-identified health information in order to re-identify the information with respect to a specific individual. Before any information is de-identified, the **Privacy Officer** will determine whether a re-identification code is necessary. In creating a re-identification code, the following requirements must be met:

i. The re-identification process must be performed in a secure manner so that no one other than the Agency can re-identify such information;

ii. The code, algorithm, table or other tool for re-identification may not be disclosed to any third-party or used for any purpose other than re-identification by the Agency; and

iii. The re-identification process utilized must be incapable of being translated or decoded by a third-party so as to identify the individual (e.g., the code cannot be a derivative of the individual's name).

The Agency requires that any re-identification code is approved by the **Privacy Officer** prior to use or disclosure. Prior to re-identification of any information, a proper plan must be developed to ensure HIPAA-compliant protection of information subsequent to re-identification.

4. Limited Data Sets

A. Limited data sets of protected health information may only be used and disclosed for research, public health, and health care operations purposes. Each limited data set must exclude all of the identifiers listed in (B) below and may only be disclosed after obtaining from the recipient a data use agreement as described in (V) below.

B. A limited data set is a set of protected health information from which all of the following direct identifiers of the individual and relatives, employers, or household members of the individual have been removed:

i. Names;

ii. Postal address information, other than town or city, State, and zip code;

iii. Telephone numbers;

iv. Fax numbers;

v. Electronic mail addresses;

vi. Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs);

vii. Internet Protocol (IP) address numbers;

viii. Biometric identifiers, including finger and voice prints; and

ix. Full face photographic images and any comparable images.

C. All individuals who wish to create a limited data set shall notify the Privacy Officer, who shall work with the individual to ensure one of the following is accomplished:

i. The individual properly removes all the identifiers listed in (B) above from the protected health information; or

ii. The individual hires an Agency-approved outside entity (with which the Agency has entered into a business associate agreement) to create the limited data set.

5. Data Use Agreement

A. Prior to disclosing a limited data set (created in compliance with the provisions of (4.) above) to any recipient, a data use agreement must be obtained from the intended recipient. The data use agreement will list the purposes for which the recipient of the limited data set can use the client information and provide the Agency with satisfactory assurance that the recipient of the limited data set will only use or disclose the client information for the purposes listed.

B. Each data use agreement must contain the following:

i. A statement indicating whether the limited data set was created for research, public health or health care operations.

ii. A statement of the purposes for which the recipient can use or disclose the client information being provided in the limited data set. These purposes must be consistent with the reason the data use set was originally created in (1).

iii. A list of the names of all individuals or entities being provided permission to receive the limited data set under the data use agreement.

iv. A statement that the recipient agrees not to use or further disclose the client information in the limited data set other than as agreed to in the data use agreement or as requirement by the law.

v. A statement that the recipient agrees to use appropriate safeguards to prevent the use or disclosure of the client information in the limited data set in any manner other than as agreed to in the data use agreement.

vi. A statement that the recipient agrees to report to the Agency if it becomes aware of any use or disclosure of the client information in the limited data set outside of the agreed upon uses in the limited data set.

vii. A statement that the recipient agrees to ensure any agents, including any subcontractors, who it provides the limited data set to will follow the same restrictions and conditions with respect to the use, disclosure and protection of the data use set.

viii. A statement that the recipient agrees to not identify the information in the limited data set or attempt to contact the individuals.

ix. A statement that the Agency can terminate the data use agreement and use of the limited data set by the recipient if it becomes aware of any pattern of behavior or activity or practice of the recipient which materially breaches or violates the data use agreement. The statement should further indicate the Agency will report any such breach or violation to the Secretary of the Department of Health and Human Services.

C. All data use agreements must be approved by the **Privacy Officer** prior to execution and disclosure of the related limited data set. We have provided a sample of a Data Use Agreement in Exhibit A.

D. The Center requires that the individual continue to comply with the Agency's minimum necessary policies, procedures and requirements in using and disclosing the client information included in the limited data set.

EXHIBIT A

FORM OF DATA USE AGREEMENT

This **Data Use Agreement**, dated as of _____, 200___ ("Agreement"), is by and between _____ ("Covered Entity") and _____ _____ ("Recipient").

WHEREAS, Covered Entity has created a Limited Data Set which contains Protected Health Information in full compliance with the Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 ("HIPAA") and related regulations promulgated by the Secretary ("HIPAA Regulations") and specifically 45 CFR § 164.514(e).

WHEREAS, Recipient desires to use and/or disclose the Protected Health Information in the Limited Data Set which was created by the Covered Entity and is subject to protection under the HIPAA Regulations.

WHEREAS, in light of the foregoing and the requirements of the HIPAA Regulations, Recipient and Covered Entity agree to be bound by the following terms and conditions:

1. **Definitions.** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E ("Privacy Rule").

A. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Recipient from Covered Entity as part of the Limited Data Set.

B. Required By Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

2. **Use and Disclosure.**

A. Purpose. Recipient agrees to not use or disclose the Protected Health Information in the Limited Data Set for purposes other than research, public health or health care operations **[Indicate Correct Purpose]** and specifically only with respect to _____ _____ _____. **[Indicate Intended Use]** The Recipient has requested inclusion of and will only utilize the following elements in the Limited Data Set:_____ _____ _____ _____. **[Indicate Specific Data Elements or Categories of Data Elements]** Recipient further agrees not to use or disclose the Limited Data Set other than as permitted or required by the this Agreement or as Required By Law.

B. Limitation. Except as otherwise limited in this Agreement, Recipient may use or disclose the Limited Data Set to perform functions, activities, or services in connection with its research, public health or health care operations function **[Indicate Correct Function]**, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

3. **Authorized Users.** The Limited Data Set shall only be used or disclosed by entities or persons authorized under this Agreement. Recipient represents and warrants that the following is a list of the persons within the Recipient that are that authorized to use or disclose the Limited Data Set:

_____

_____

4. **Agents.** Recipient agrees to ensure that any agent, including a subcontractor, to whom it provides the Limited Data Set, agrees to the same restrictions and conditions that apply through this Data Use Agreement to Recipient with respect to such information. Recipient further agrees that each such agent shall enter into a Data Use Agreement substantially similar to this Agreement.

5. **Appropriate Safeguards.** Recipient agrees to use appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as provided for in this Agreement. Without limiting the generality of the foregoing, Recipient agrees to protect the integrity and confidentiality of any Protected Health Information it electronically exchanges with Covered Entity.

6. **Reporting.** Recipient agrees to report to Covered Entity any use or disclosure of the Limited Data Set not provided for by this Agreement of which it becomes aware.

7. **Protection of Individuals**. The Recipient agrees that it will not identify any of the Protected Health Information provided to it in the Limited Data Set nor will it attempt to contact the individuals whose Protected Health Information is included in the Limited Data Set.

8. **Permissible Requests by Covered Entity**. Covered Entity shall not request Recipient to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule, if done by Covered Entity.

9. **Term and Termination.**

A. Term. This Agreement shall be effective as of the date set forth above, and shall terminate when all of the Limited Data Set provided by Covered Entity to Recipient, or created or received by Recipient on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy the Limited Data Set, protections are extended to such information, in accordance with the termination provisions in this Section.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Recipient, Covered Entity shall either:

i. Provide an opportunity for Recipient to cure the breach or end the violation. If Recipient does not cure the breach or end the violation within the time specified by Covered Entity, Covered Entity shall terminate this Agreement;

ii. Immediately terminate this Agreement if Recipient has breached a material term of this Agreement and cure is not possible; or

iii. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of the Department of Health and Human Services.

C. Effect of Termination.

i. Except as provided in paragraph ii. of this Section 9.c., upon termination of this Agreement, for any reason, Recipient shall return or destroy the Limited Data Set and all Protected Health Information received from Covered Entity, or created or received by Recipient on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Recipient. Recipient shall retain no copies of the Limited Data Set or any other Protected Health Information.

ii. In the event that Recipient determines that returning or destroying the Limited Data Set and the Protected Health Information is infeasible, Recipient shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the Limited Data Set and Protected Health Information is infeasible, Recipient shall extend the protections of this Agreement to such Limited Data Set and all Protected Health Information and limit further uses and disclosures of such Limited Data Set and all Protected Health Information included therein to those purposes that make the return or destruction infeasible, for so long as Recipient maintains such Limited Data Set.

10. Miscellaneous.

A. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

B. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA.

C. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

D. Miscellaneous. This Agreement constitutes the entire agreement between the parties with respect to the subject matter contained herein.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date set forth above.

Catholic Charities of the Diocese of Long Island	**[INSERT NAME OF RECIPIENT]**
By: _____	By: _____
Name:	Name:
Title:	Title:

HIPAA PRIVACY TOOL #9

CATHOLIC CHARITIES
(the "Agency")

SUBJECT: **Facsimile Transmissions of Health Information**

REFERENCES: **45 CFR § 164.530; DHHS Privacy Guidance, July 6, 2001**

EFFECTIVE DATE: **April 1, 2003**

APPROVED BY:

PURPOSE. The Agency has adopted this policy to protect the confidentiality of client health information and privacy of facsimile transmissions.

GENERAL POLICY. Facsimile transmissions of client information are permissible provided that the requirements for disclosure of client health information are met (for a description of these requirements, see policy titled *"Uses and Disclosures of Patient Information for Various Legal, Public Health, Regulatory and Employment Purposes Policy"*). Employees should be aware that the use of fax machines poses a heightened risk of unauthorized disclosure of client information. In order to protect client confidentiality and reduce the risk of unauthorized receipt of facsimile transmissions, the Agency has implemented the additional safeguards and verification procedures discussed in this policy.

PROCEDURES.

1. **Verify Requestor**. In many instances the identity of the individual requesting the facsimile transmission is already known to the program. However, if the program representative is unfamiliar with the requestor, he/she should call back the requestor to verify his/her status and identity. Even if the identity of the requestor is known, the program should, when reasonable, verify that the requestor has a legitimate right to receive the client health information which was requested.

2. **Ensure appropriate documentation**. Disclosure of client health information for treatment, payment or healthcare operations is generally permissible, subject to the Agency's HIPAA Privacy Notice (see policy titled, *"HIPAA Privacy Notice"* for additional information). Disclosure of this information for most other purposes requires the client to sign a client authorization. Before sending a facsimile transmission, it should be verified that the Agency has a copy of the necessary documentation to release the information requested. For a more thorough discussion regarding the documentation requirements for release of client information see the policy titled *"Uses and Disclosures of Patient Information for Various Legal, Public Health, Regulatory and Employment Purposes"*. If the Agency is unable to confirm the client's authorization, when required, the Agency will call the client to obtain a written authorization for such disclosure and/or require the requestor to obtain such written authorization.

3. **Verify the Fax Number.** Before sending a facsimile transmission, the sender must verify that the fax number listed is the correct fax number for the recipient. The sender should double check the recipient's fax number entered into the fax machine before pressing the send key. Where possible, program your fax machine with known fax numbers. If the fax number has been pre-programmed into the fax machine, at least one test fax should be sent before relying on this number to fax client health information.

4. **Call Intended Fax Recipient Before Sending Client Health Information.** When reasonable, the sender should contact the recipient of the client information to ensure that the recipient knows that the fax is coming and arrange for its timely pick up from the fax machine.

5. **Legend on Fax Cover Required** All facsimile transmissions being sent by the Agency must be accompanied by a fax cover sheet that includes the following confidentiality legend in large bold type:

> **CONFIDENTIAL COMMUNICATION**
>
> **THIS TRANSMISSION IS INTENDED ONLY FOR THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND CONTAINS INFORMATION THAT IS CONFIDENTIAL. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE DESTROY THE FAXED MATERIALS AND CONTACT THE SENDER IMMEDIATELY AT THE NUMBER STATED ABOVE.**
>
> **THIS INFORMATION IS CONFIDENTIAL AND MAY BE PROTECTED BY FEDERAL AND/OR STATE LAW. IN THAT CASE, FEDERAL AND/OR STATE LAW PROHIBITS YOU FROM MAKING ANY FURTHER DISCLOSURE OF THIS INFORMATION. ANY UNAUTHORIZED FURTHER DISCLOSURE IN VIOLATION OF THE LAW MAY RESULT IN SUBSTANTIAL PENALTIES. IF THE READER OF THIS COMMUNICATION IS NOT THE INTENDED RECIPIENT, OR ITS EMPLOYEE, OR AGENT RESPONSIBLE FOR DELIVERING THE COMMUNICATION TO THE INTENDED RECIPIENT, YOU ARE NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED.**

6. **Send Only Minimum Necessary Information**. Only the information requested should be sent in the facsimile transmission (see policy titled *"The Minimum Necessary Rule Under the Privacy Regulations"*).

7. **Confirmation of Delivery.** The sender of the fax must check the fax transmittal summary, log and/or fax confirmation sheet to ensure that the fax was sent to the correct recipient(s). If the sender determines that the fax was erroneously received by an unauthorized recipient, the employee must take steps to immediately contact the unintended recipient and ask that the fax be destroyed. The employee also must document the erroneous transmission, record the date and events, and inform his/her supervisor of the error.

8. **Random Verification of Receipt of Facsimiles**. On a random basis the program should call the recipient of the fax, after the fax has been sent, to ensure that the appropriate person has received the information.

9. **Update Fax Numbers.** The program will request updated fax numbers from its regular fax recipients, such as referral sources, and notify all relevant departments of the new fax number.

AUTO FACSIMILE TRANSMISSION DIRECTLY FROM THE COMPUTER. When using the auto-fax function directly from a computer (e.g., facsimile transmission of summary progress reports or case management summaries), the sender must comply with the procedures provided above, where applicable. In addition, the following safeguards should be implemented:

1. **Fax Cover Sheet**. If possible, the computer should be programmed to have each facsimile transmission accompanied by a cover sheet with the language provided in item # 5 above.

2. **Routine Review of Confirmation Logs**. The sender or a program representative, should routinely review any computerized logs of transmissions (or other confirmation provided) to ensure that the fax was sent to the intended recipient(s).

3. **Update Fax Numbers**. As noted above, the programmed list of fax numbers should be routinely updated. Any facsimile numbers which have been disabled or altered should be promptly corrected in the computerized listing of fax numbers.

SECURITY MEASURES.

Fax machines should be located in a private and secure area. The fax machines utilized for sending and receiving facsimiles should be located in areas that are secure, and not accessible to the public. Access to these areas should be limited and require security keys, badges and/or other proper Agency identification. When reasonable, an employee or employees should be designated to periodically check the fax machine to assure that faxes containing client information are not left unattended in the machine.

Remove Paper from the Machine. If a fax machine is designated to receive sensitive transmissions during off-shifts (i.e., overnight) and the area is not secured, each program or department should consider removing paper from the machine each night, so that facsimiles will not print until an authorized individual is available to retrieve the information.

HIPAA PRIVACY TOOL #10

CATHOLIC CHARITIES
OF LONG ISLAND

AUTHORIZATION FORM FOR THE RELEASE OF CLIENT INFORMATION

Section A: Must be completed for all authorizations

I hereby authorize the use and disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I also understand that if a person or organization authorized to receive my information is not a health plan or health care provider, the released information may be subject to redisclosure and may no longer be protected by the federal privacy regulations.

Client name:	ID Number (if applicable):
Persons/organizations authorized to use or disclose my information:	Persons/organizations who may receive my information:

Specific description of the information to be used or disclosed (including date(s)):

Description of each purpose of the use or disclosure of my health information: (Note: If the release of information is requested by the client, please insert "at the request of the client" here if the client does not provide a statement of purpose.)

For marketing authorizations only: Does the marketing for which this authorization is being requested involve direct or indirect remuneration from a third party to the Agency?

Section B: The client or the client's representative must read and initial the following statements

1. I understand that this authorization will expire on _____ Initials
   [Insert Expiration Date or Event]

2. I understand that I may refuse to sign this form and that my health care and the payment for my health care will not be affected if I do not sign this form. Initials

3. I understand that I will get a copy of this form after I sign it. Initials

4. I understand that I may revoke this authorization at any time by notifying the Agency in writing, but if I do, the revocation will not have any effect on actions the Agency has already taken in reliance on this authorization. Initials

_____ _____

Signature of client or client's representative **Date**

(Note: *This form MUST be completed before signing.)*

If this authorization is signed by a client's representative, please complete the following:

_____

Printed name of client's representative:

_____

Relationship to the client:

Describe the representative's authority to act for the client:

_____

_____

_____

** YOU MAY REFUSE TO SIGN THIS AUTHORIZATION **

Catholic Charities of Long Island

AUTHORIZATION/CONSENT FOR USE OR DISCLOSURE OF INFORMATION FOR PUBLICATION PURPOSES

Part I. Name of Service Recipient:	
Name: Last First MI	*Last 4 Digits of Social Security Number*
Address:	*Date of Birth:* *Phone Number:* ( )

Part II. Authorization for Use and Disclosure of Information, including Protected Clinical Information:

I, the undersigned, hereby authorize Catholic Charities and its affiliates, employees and agents (collectively, "Catholic Charities") to photograph, film and/or record the Service Recipient (referred to as the "Recording") and use and disclose the Recording and my information to the public as indicated below. I acknowledge that I have been informed that I, my physician or Catholic Charities of Long Island staff may request that the Recording be stopped at any time, even if the Recording has not been completed, and such Recording shall immediately cease.

The following information about the Service Recipient may be used by Catholic Charites [check all that apply]:

- ☐ Name and health information
- ☐ The Recording
- ☐ Other protected health information [describe]: _____

For the purpose described below:

I agree to the usage described below: [check all that apply]

- ☐ Posting on the Catholic Charities Internet Website
- ☐ Publication in a Catholic Charities Newsletter or other format for public distribution
- ☐ Catholic Charities Training materials
- ☐ Social Media in any form
- ☐ News outlets, both print and video
- ☐ All of the above
- ☐ Other (Please describe):

Please list exceptions below.

_____

_____

This authorization shall expire ten years after the Service Recipient ceases being a service recipient of the Catholic Charities, unless I indicate another termination date or event here:

_____

Part III. Signature and Date:

1. I understand that I will not receive any payment or compensation for the use or disclosure of the Recording or my other information.
2. Catholic Charities will not receive compensation in exchange for using or disclosing my PHI or the Recording.
3. I may revoke this authorization, in writing, at any time by immediately notifying Catholic Charities. I understand that a revocation is not effective against actions taken by Catholic Charities before they received such revocation and to the extent that they relied upon this authorization.
4. I understand that if the person or entity authorized to receive my health and/or clinical information is not a health care provider or health plan, the released information may be re-disclosed and may no longer be protected by federal privacy regulations.
5. There is no requirement to sign this form authorizing the release of protected health information and refusal to sign will not affect my ability to obtain treatment except in some situations when such information is needed for payment and enrollment.
6. I may, in accordance with any applicable agency Privacy Policy, inspect or copy any information used or disclosed under this authorization upon request and obtain a copy of this form if I ask for it.
7. I hereby irrevocably release Catholic Charities and affiliates from, and waive, any and all claims, damages or rights of whatever kind that I or the Service Recipient may have or may later assert (at law, in equity or otherwise) against Catholic Charities and affiliates related in any way to the (1) use or disclosure of the Recording or the Service Recipients information as authorized herein; or (2) the cessation of the Recording.

_____ _____

Signature of Individual or Representative *Date*

_____ _____

Print Name of Individual or Representative *Representative's Relationship to Individual*

A copy of this signed form shall be provided to the Individual or Representative

PRIVACY TOOL # 11

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **MARKETING**

REFERENCES: **45 CFR § 164.501 AND 45 CFR § 164.508(a)(3)**

EFFECTIVE DATE: September 22, 2013

APPROVED BY:

Purpose: The purpose of this Policy and Procedure is to ensure that the Agency is in compliance with HIPAA's requirements regarding marketing. The Agency's goal is to safeguard the confidentiality and integrity of Client information and to protect against the unauthorized access to, or release of such information.

HIPAA has specific rules about when the Agency can use Client information (including the name, address, dates of service, or medical information of a Client) for marketing. When using Client information for marketing, the Agency will take the following steps:

STEP 1: DETERMINE IF THE COMMUNICATION IS MARKETING

A. Definition and Exceptions.

HIPAA defines "Marketing" broadly as any communication (oral or written) about a product or service that encourages the recipients of the communication to purchase or use the product or service.

1. The following are considered to be exceptions to the Marketing definition, regardless of whether there is Financial Remuneration, as defined below, in exchange for the communication:

a) a face-to-face communication between Agency personnel and the Client;

b) Promotional gifts to the Client of nominal value provided by the Agency (e.g., the Agency can distribute pens, toothbrushes, or key chains with the name of the Agency on them).

2. In addition, the following communications are considered to be made for health care operations or treatment purposes, and not Marketing, as long as Financial Remuneration, as defined below, is not received from a third party in exchange for the Agency communicating about the third party's services or products:

a.) Describing a health-related product or service (or payment for such product or service) that is provided by the Agency, including communications about:

i. The entities participating in a health care provider network or health plan network;

ii. Replacement of, or enhancements to, a health plan; or

iii. Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

b.) Communications about treatment of an individual.

c.) Case management or care coordination.

d.) Contacting a Client with information about treatment alternatives and related functions to the extent these activities do not fall within the definition of treatment.

e.) Communications that merely promote health in a general manner and do not promote a specific product or service.

f.) Communications to promote health fairs, wellness classes, support groups, and population-based activities to improve health or reduce health costs.

g.) Sending information about government and government-sponsored programs (e.g., Medicaid, Medicare, etc.).

For the communications listed in Item 2, the rules for using or disclosing PHI for health care operations or treatment purposes should be followed (e.g., a Client authorization is generally not required in order to make such communications).

B. Financial Remuneration.

1. "Financial Remuneration" means direct or indirect payment to the Agency or its Business Associate from or on behalf of a third party whose product or service is being described in exchange for making a communication about the third party's product or service (i.e., to qualify as financial remuneration, the remuneration must be for the purpose making the communication).

   Example: If a third party provides Financial Remuneration to an Agency in order for the Agency to develop a disease management program, the Agency can use PHI to inform Clients about the Agency's disease management program because the Financial Remuneration was not received in exchange for making the communication and the communication was not about the third party's products or services (i.e., the communication is about the Agency's disease management program). In comparison, if a third party provides Financial Remuneration in order for the Agency to inform its Client's about the third party's disease management program, this would be considered Marketing and Client authorization would be required to use or disclose the Client information.

2. Financial Remuneration does not include non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for making a communication about a product or service.

3. The Agency may provide refill reminders or communications about a drug or biologic currently being prescribed for the individual, even if Financial Remuneration is exchanged, provided that the Financial Remuneration provided in exchange for making the communication is reasonably related to the Agency's cost of making the communication (the costs of labor, supplies and postage to make the communication) and does not provide the Agency with a profit.

4. If Financial Remuneration is otherwise received by the Agency in exchange for making a communication about a third party's services or products, even if the communication would otherwise be considered to be health care operations or treatment as discussed in Section A.2 above, the communication is considered to be Marketing, and Step 2 below needs to be followed.

C. Determination of Not Marketing. If it is determined that the communication is not Marketing because one of the exceptions is met and no prohibited Financial Remuneration is received, PHI can be used to make the communication consistent with the Agency's policies regarding health care operations and treatment.

STEP 2: OBTAIN CLIENT AUTHORIZATION

If it is determined in that a communication falls within the HIPAA definition of Marketing and: (A) does not fall within any of the exceptions described above A.1; and (B) is not considered to be health care operations or treatment as discussed in A.2, the Agency must obtain the Client's written HIPAA authorization prior to using or disclosing the Client's information for Marketing. If Marketing involves direct or indirect Financial Remuneration to the Agency from a third party, the authorization must state that the Agency is receiving such Financial Remuneration.

Note: The Agency may not give away or sell lists of Clients for Marketing purposes without obtaining a HIPAA authorization from each Client on the list. If the Agency engages a business associate to assist the Agency with Marketing (e.g., a telemarketer), the Agency will require compliance (by the business associate) with all applicable HIPAA rules regarding marketing.

STEP 3: OBTAIN ADVICE IF UNSURE

In certain circumstances, it may be difficult to determine whether a particular communication is considered Marketing. Any questions regarding Marketing issues should be reviewed by the Agency's Privacy Officer prior to making the communication.

HIPAA PRIVACY TOOL #12

CATHOLIC CHARITIES

(the "Agency)

POLICY & PROCEDURE

SUBJECT:	**FUNDRAISING**
REFERENCES:	**45 CFR 164.501, 45 CFR 164.514(f)**
EFFECTIVE DATE:	September 22, 2013
APPROVED BY:	

The purpose of this Policy and Procedure is to ensure that the Agency is in compliance with HIPAA's requirements regarding Fundraising. The Agency's goal is to safeguard the confidentiality and integrity of Client information and to protect against the unauthorized access, disclosure, or release of such information.

HIPAA has specific rules about when the Agency can use Client information for fundraising. When using such Client information for fundraising, the Agency will take the following steps:

A. Step One: Determine Whether Fundraising Can Occur Without an Authorization.

Client information can be used for fundraising activity, without an authorization, so long as the following criteria are met:

1. The Agency's Privacy Notice must include a statement in the body of the notice that the Agency may contact the individual to raise funds for the Agency and that the individual has a right to opt out of receiving such communications.

2. The Client information used is limited to the Client's demographic information (i.e., the Client's name, address, contact information, age, gender and date of birth), dates of service, department of service information, treating physician, outcome information, and health insurance status.

3. The fundraising activity must be intended to solely benefit the Agency.

4. The Client information must be used directly by the Agency or, on behalf of the Agency, by a:

    a. Business Associate of the Agency (pursuant to a Business Associate Agreement with the Agency), or

    b. foundation that has in its charter statement of charitable purposes an explicit linkage to the Agency, for the purpose of raising funds for the Agency.

5. The Agency must include in each fundraising communication a clear and conspicuous description of how the Client may opt out of receiving any further fundraising communications. The method for the Client to opt out must not cause an undue burden or involve more than a nominal cost. Acceptable opt out procedures include having the Client contact a toll free number or email address. Requiring a Client to write and send a letter to the Agency is an unacceptable opt out procedure. The Agency must institute procedures to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications. Notwithstanding the foregoing, the Agency may institute a policy and procedure that allows individuals who have previously opted out from receiving fundraising communications to opt back in to receiving such communications.

6. The Agency may not condition treatment or payment on a Client's choice with respect to receiving fundraising communications.

Step Two: If Necessary, Obtain a HIPAA Authorization From the Client.

For fundraising communications that do not fit the criteria set forth in Step One, the Agency must obtain the Client's written HIPAA authorization prior to using the Client's health information in a fundraising communication.

PRIVACY TOOL # 14

CATHOLIC CHARITIES

(the "Agency")

POLICY & PROCEDURE

SUBJECT: **Client Request Not to Disclose PHI to a Health Plan**

REFERENCES: **45 CFR § 164.522**

EFFECTIVE DATE: **September 22, 2013**

APPROVED BY:

PURPOSE

This Policy and Procedure establishes the rules that the Agency will follow when a Client requests that the Agency not disclose his/her protected health information ("PHI") or submit a claim for services rendered to his/her health plan.

POLICY

A Client has the right to request restrictions on how the Agency uses or discloses the Client's PHI to carry out treatment, payment and health care operations. The Agency must agree to a Client request to restrict disclosure of PHI to a health plan if: a) the PHI pertains solely to health care items or services for which the Client has paid the Agency in full at time of service; and b) the disclosure is not otherwise required by law (e.g., responding to a Medicare or Medicaid audit).

The restriction on disclosure of PHI to a health plan will not apply to follow-up treatment if disclosure of the original treatment information is necessary to receive payment for the follow-up treatment, UNLESS the Client requests that the follow-up (and original) treatment information not be disclosed to the health plan and the Client pays for the follow-up treatment in full as described herein

PROCEDURE

1. If a Client requests that the Agency not submit his/her PHI to his/her health plan for services rendered, the Client must make the request to the Site Coordinator in writing on the attached form (Client Restriction on PHI Disclosure). The request will only be honored if the Client pays the Agency, in full, for the care. For elective services, an initial payment of estimated charges will be required to be made up front prior to receipt of services and any outstanding amounts due will need to be paid within thirty (30) days of the receipt of an invoice from the Agency. In the case of an emergency, payment for emergency services will need to be made within thirty (30) days of receipt of an invoice from the Agency.

Note: Where the restriction requested by the Client applies only to one of several services provided during a single Client encounter, the Client must agree to pay for all the services provided if the services cannot be unbundled.

2. The Site Coordinator will document the request for restriction in the Client's Chart

3. If payment is not received within thirty days of Client's discharge, one written reminder will be sent to the Client and if the Client does not submit or make arrangements for payment within three (3) business days, the Agency may submit a claim to the health plan for payment. Furthermore, if the Client make the payment and the Client's payment is subsequently dishonored (e.g., a check is returned for insufficient funds), the Agency will notify the Client in writing that payment was not obtained and that the Client has three (3) business days to remit payment. If payment is not received within three (3) business days, the Agency may submit a claim to the health plan for payment.

3. The Agency does not need to maintain a separate medical record for services where the Client has requested that his/her health plan not be billed, but the Agency will flag the record to indicate that a restriction has been placed on disclosure.

4. All requests for restrictions will be referred to the Site Coordinator.

CATHOLIC CHARITIES

Client Restriction on PHI Disclosure

Client Name	Date of Birth

I request that health information regarding my (the Client's) care and treatment received on _____ ("Services") NOT be released by the Agency to my health plan: _____ ("Health Plan"). As a result of this restriction, I understand that the Agency will not submit any claim for payment for the Services to the Health Plan, and I agree to be financially responsible for cost of and to reimburse the Agency in full for the Services. I understand that I must make an initial payment of $ _____. Any subsequent amounts due must be paid within thirty (30) days of discharge.

I understand that if the Agency is not paid in full within 30 days of discharge, the Agency is permitted to submit a claim to my health plan for the Services.

I further understand that this restriction on disclosure of my health information does not apply to any follow-up care I receive, unless I specifically request that information about the follow-up care also not be provided to the health plan. I understand that such request must be made at the time I receive the follow-up care, and if I make such request, I will also be responsible for payment, in full, for the follow-up care.

I acknowledge that this request does not apply to related services that are not provided by the Agency (e.g., pharmacy, durable medical equipment) and that I will need to make separate requests to such providers if I do not want them to release my information to my health plan.
All items on this form have been completed and my questions about this form have been answered. In addition, I have been provided a copy of the form.

_____ Signature of Client or Personal Representative	Date: _____

HIPAA PRIVACY TOOL #15

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **THE MINIMUM NECESSARY RULE UNDER THE PRIVACY REGULATIONS**

REFERENCES: **45 CFR §§ 164.502(b), 164.514(d)**
DHHS Privacy Guidance, July 6, 2001

EFFECTIVE DATE: **April 1, 2003**

APPROVED BY:

1. INTRODUCTION

The purpose of this Policy and Procedure is to ensure that the Agency is in compliance with the requirements of the minimum necessary rule. The minimum necessary rule generally requires that, when using, disclosing or requesting client information, the Agency take reasonable steps to limit the client information to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. For example, if the Agency discloses client information for the purpose of receiving payment for services rendered, the amount of client information disclosed should be limited to the minimum amount necessary to receive payment.

The minimum necessary rule **does not** apply to:

A. **Disclosures** to or **requests** by a health care provider for **treatment** purposes (**Note**: The rule **does** apply to **uses** of client information for **treatment** purposes);
B. Disclosures to the individual who is the subject of client information;
C. Uses or disclosures made pursuant to an authorization;
D. Uses or disclosures required for compliance with HIPAA's privacy standards;
E. Disclosures to the Department of Health and Human Services when disclosures of client information are required under the Privacy Rules; and
F. Uses or disclosures that are required by other laws.

2. USES OF CLIENT INFORMATION

Listed in Exhibit A are the names of various classes of Agency employees who require access to the Agency's client information to carry out their duties. The Agency will make reasonable efforts to limit the

access of its personnel to the client information they are entitled to receive (as described in Exhibit A). Only those individuals with a "need to know" should have access to client information.

3. ROUTINE OR RECURRING DISCLOSURES OF CLIENT INFORMATION

For disclosures of client information which are routine or recurring, the Agency will take the following steps to limit the client information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure:

Examples of steps to implement the minimum necessary rule:

A. Locking file cabinets or records rooms with client information after business hours;
B. Implementing security procedures for computers to limit access to client information (e.g., passwords); and
C. Limiting access to medical records areas to authorized personnel.

The Agency will not make a detailed determination about the proprietary of each and every routine or recurring disclosure. Additionally, the Agency will rely, if reliance is reasonable under the circumstances, on the assumption that a requested disclosure meets the minimum necessary rule in the following circumstances:

- Public Officials: When making disclosures to public officials as permitted by the Privacy Regulations, if the public officials represent that the information requested is the minimum amount necessary;

- Other Covered Entities: When making disclosures of information to other HIPAA covered entities, including other providers or health plans or health care clearinghouses (e.g., billing companies);

- Professionals: When the information is requested by professionals (e.g., lawyers or accountants) who are members of the Agency's workforce or business associates for the purpose of providing professional services to the Agency, if each professional represents that the information requested is the minimum amount necessary; or

- Researchers: When a person requests protected health information for research purposes so long as the person has provided documentation or representations that applicable HIPAA requirements regarding the use of protected health information for research purposes have been met.

The Agency will not disclose an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the disclosure or when such a disclosure is described as permissible in Exhibit B. Since disclosures of PHI made for treatment purposes are exempt from the minimum necessary rule, disclosures of the entire medical record for this purpose are acceptable.

4. ROUTINE OR RECURRING REQUESTS FOR CLIENT INFORMATION

For the routine or recurring requests for client information which the Agency makes to other health care providers, health plans or health care clearinghouses (e.g., billing companies), the Agency will take the

following steps to limit the client information requested to the amount reasonably necessary to achieve the purpose of the request:

A. Keeping a log of requests for client information; and

B. Conducting random audits of access to client files to verify that unauthorized or over-broad requests are not made.

The Agency will not make a detailed determination about the proprietary of each and every routine or recurring request for client information. Additionally, the Agency will not request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the request or when such a request is described as permissible in Exhibit C. Since requests for PHI made for treatment purposes are exempt from the minimum necessary rule, requests for the entire medical record for this purpose are acceptable.

5. NON-ROUTINE OR NON-RECURRING DISCLOSURES OR REQUESTS FOR CLIENT INFORMATION

For non-routine or non-recurring disclosures of or requests for client information, the Agency must review each disclosure or request on a case-by-case basis. In addition, each non-routine or non-recurring disclosure of or request for an entire medical record must also be reviewed on a case-by-case basis. In each instance, the Agency must determine whether the minimum amount of client information is being disclosed or requested. The criteria which the Agency will consider in evaluating each disclosure or request will include:

[The Agency should insert the criteria it will consider for each non-routine disclosure or request. Criteria must be designed to limit the client information requested or disclosed to the minimum amount necessary. For disclosures of or requests for the entire medical record, the Agency should specify any specific criteria it will consider for this type of disclosure or request. Suggested criteria include:

i. The purpose of the disclosure/request;

ii. The type of client information to be disclosed or requested;

iii. The minimum amount of client information necessary to achieve the purpose of the disclosure or request;

iv. For disclosures, the amount of client information requested for disclosure (Note: Does it include the entire medical record?);

v. The individuals/entities to whom a disclosure or request will be made;

vi. The time frame for the disclosure or request; and

vii. Any specific client considerations.]

Additionally, the Agency will document its individualized review of non-routine or non-recurring disclosures of or requests for PHI.

For non-routine or non-recurring disclosures of an entire medical record, the Agency's staff will document each instance in which an entire medical record is disclosed and will describe the bona fide reasons why the entire medical record is necessary (See the form attached as Exhibit D). For non-routine or non-recurring requests, the Agency's staff will document each instance in which an entire medical record is requested and will describe the bona fide reasons why the entire medical record is necessary (See the form attached as Exhibit D). However, disclosures of and requests for an entire medical record for treatment purposes do not have to be documented.

6. ENFORCEMENT

The Agency will make reasonable efforts to limit the access of its employees to the client information they are entitled to access. In addition, the Agency will make reasonable efforts to enforce the minimum necessary rule and the policies described in this policy. The Agency will update this policy as necessary to reflect any changes made from time to time (including changes in staff).

EXHIBIT A

USES OF CLIENT INFORMATION

Class of Employees[8]	Types of Client Information Used[9]	Conditions on Access (If Any)[10]
Example: Therapists	Medical records relating to the clients they treat as well as other records relating to the medical services each therapist provides (e.g., billing records, quality assurance records, etc.)	Therapists should only have access to client records for the clients they treat. Therapists may access entire medical records when necessary for the treatment of the client.

[8] **Note**: The Agency should specify various classes of employees who require access to client information (e.g., therapists, clerical staff, billing staff, etc.).

[9] **Note**: The Agency should list each category of information to which an employee has access (e.g., medical information, billing records, etc.). If an individual requires access to entire medical records, this access must be indicated and a justification should be included.

[10] **Note**: The Agency should indicate whether, for a particular individual, there are any conditions on access. For example, billing staff may only have access to client information when they are preparing a bill.

EXHIBIT B

ROUTINE OR RECURRING DISCLOSURES OF ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Disclosure[11]	**Justification**[12]	**Conditions on Disclosure (If Any)**[13]
Example: Disclosures to payors to prove medical necessity for health care claims.	Disclosure of the entire medical record is necessary to substantiate health care claims. The Agency is entitled to rely on health plans to request only the minimum amount of client information necessary.	Disclosures of the entire medical record will only be made to payors when payors request disclosure of the entire medical record. Disclosures will not be made if, in the Agency's judgment, a request for disclosure is unreasonable.

[11] **Note:** The Agency should identify the type of disclosure as well as the individuals or entities (or classes of individuals or entities) to whom the disclosure is routinely made.

[12] **Note:** The Agency should describe the reasons why disclosure of the entire medical record is appropriate.

[13] **Note:** The Agency should indicate whether there are any conditions on disclosures.

EXHIBIT C

ROUTINE OR RECURRING REQUESTS FOR ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Requests[14]	Justification[15]	Conditions on Disclosure (If Any)[16]
Example**:** Requests for entire medical records from other providers for payment purposes.	The entire medical record is necessary to substantiate health care claims.	Requests for entire medical records will only be made when the Agency's staff make the determination that the entire medical record is necessary to justify health care claims.

[14] **Note**: The Agency should identify the type of request as well as the individuals or entities (or classes of individuals or entities) to whom the request is routinely made.

[15] **Note**: The Agency should describe the reasons why disclosure of the entire medical record is appropriate.

[16] **Note**: The Agency should indicate whether there are any conditions on disclosures.

EXHIBIT D

LOG OF NON-ROUTINE OR NON-RECURRING DISCLOSURES OF OR REQUESTS FOR AN ENTIRE MEDICAL RECORD

Date of Disclosure/Request	Client Information Disclosed or Requested	Persons/Entities Who Received the Disclosure/Request	Justification

EXHIBIT A

ADDICTION TREATMENT SERVICES

USES OF CLIENT INFORMATION

Class of Employees	Types of Client Information Used	Conditions on Access (If Any)
Director **Medical Director** **Program Coordinator** **Clinic Coordinator** **Clinic Supervisor** **Clinical Supervisor** **Counselors** **Direct Care Staff** **Registered Nurses** **Licensed Practical Nurses**	Medical records relating to the clients they treat as well as other records relating to the medical services each therapist provides (e.g., billing records, quality assurance records, etc.)	Counselors should only have access to client records for the clients they treat. Counselors may access entire medical records when necessary for treatment of the client.
Billing Support Staff **Receptionist/Secretary** **Office Manager**	Medical records relating to the clients they treat as well as other records relating to the medical services each therapist provides (e.g., billing records, quality assurance records, etc.)	Only information needed for insurance and billing
Drivers	Clients' name, address, & phone number only	No access to client charts

EXHIBIT B

ADDICTION TREATMENT SERVICES
ROUTINE OR RECURRING DISCLOSURES OF ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Disclosure	Justification	Conditions on Disclosure (If Any)
Disclosures to payers to prove medical necessity for health care claims. i.e., Insurance companies, etc.	Disclosure of the entire medical record is necessary to substantiate health care claims. The Agency is entitled to rely on health plans to request only the minimum amount of client information necessary.	Disclosures of the entire medical record will only be made to payers when payers request disclosure of the entire medical record. Disclosures will not be made if, in the Agency's judgment, a request for disclosure is unreasonable.
OASAS Auditors	Inspection to insure compliance with Regulations	Must be requested by governmental official
Legal Referrals	As a condition of treatment per signed release by client	Must be requested by governmental official

EXHIBIT C

ADDICTION TREATMENT SERVICES
ROUTINE OR RECURRING REQUESTS FOR ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Requests	Justification	Conditions on Disclosure (If Any)
Requests for entire medical records from other providers for payment purposes.	The entire medical record is necessary to substantiate health care claims.	Requests for entire medical records will only be made when the Agency's staff makes the determination that the entire medical record is necessary to justify health care claims.

EXHIBIT D

ADDICTION TREATMENT SERVICES
LOG OF NON-ROUTINE OR NON-RECURRING
DISCLOSURES OF REQUESTS FOR AN ENTIRE MEDICAL RECORD

Date of Disclosure/Request	Client Information Disclosed or Requested	Persons/Entities Who Received the Disclosure/Request	Justification

EXHIBIT A

SIENA RESIDENCE

USES OF CLIENT INFORMATION

Class of Employees[17]	Types of Client Information Used[18]	Conditions on Access (If Any)[19]
Program Coordinator of Siena Residence		Only records of Siena clients.
Residence Manager	All client records	Only records of Siena clients.
Residential Counselors	Client Medical Records	Only clients they are assigned.
Interns	Client Medical Records	Only clients they are assigned.
Secretary	Client Billing Records	Only clients they are assigned.

[17] **Note:** The Center should specify various classes of employees who require access to client information (e.g., therapists, clerical staff, billing staff, etc.).

[18] **Note:** The Center should list each category of information to which an employee has access (e.g., medical information, billing records, etc.). If an individual requires access to entire medical records, this access must be indicated and a justification should be included.

[19] **Note:** The Center should indicate whether, for a particular individual, there are any conditions on access. For example, billing staff may only have access to client information when they are preparing a bill.

EXHIBIT B

SIENA RESIDENCE

ROUTINE OR RECURRING DISCLOSURES OF ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Disclosure[20]	Justification[21]	Conditions on Disclosure (If Any)[22]
Disclosures to payors to prove medical necessity for health care claims.	Disclosure of the entire medical record is necessary to substantiate health care claims. The Center is entitled to rely on health plans to request only the minimum amount of client information necessary.	Disclosures of the entire medical record will only be made to payors when payors request disclosure of the entire medical record. Disclosures will not be made if, in the Center's judgment, a request for disclosure is unreasonable.
New York State Office of Mental Health	Disclosure of entire records is necessary for oversight and re-certification.	No conditions.
Medicaid	Disclosure of entire records is necessary to receive payment for services.	Disclosure of entire medical records will only be allowed when request for disclosure is made.
SSI/SSD	Disclosure of entire records is necessary to certify client is disabled and is receiving required services.	Disclosure of entire medical records will only be allowed when request for disclosure is made.

[20] **Note:** The Center should identify the type of disclosure as well as the individuals or entities (or classes of individuals or entities) to whom the disclosure is routinely made.

[21] **Note:** The Center should describe the reasons why disclosure of the entire medical record is appropriate.

[22] **Note:** The Center should indicate whether there are any conditions on disclosures.

EXHIBIT C

SIENA RESIDENCE

ROUTINE OR RECURRING REQUESTS FOR ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Requests[23]	**Justification**[24]	**Conditions on Disclosure (If Any)**[25]
Requests for entire medical records from other providers for payment purposes.	The entire medical record is necessary to substantiate health care claims.	Requests for entire medical records will only be made when the Center's staff makes the determination that the entire medical record is necessary to justify health care claims.
New York State Office of Mental Health	Disclosure of entire records is necessary for oversight and re-certification.	No conditions.
Medicaid	Disclosure of entire records is necessary to substantiate health care claims.	Disclosure of entire medical records will only be allowed when request for disclosure is made.
SSI/SSD	Disclosure of entire records is necessary to certify client is disabled and is receiving required services.	Disclosure of entire medical records will only be allowed when request for disclosure is made.
S.P.O.A./S.P.A.	Medical records regarding appropriate placement.	Disclosure of necessary records after receiving signed consents.
Mental Health Clinics	Medical records regarding treatment progress.	Disclosure of necessary records after receiving signed consents.
School Districts	Medical records regarding treatment progress.	Disclosure of necessary records after receiving signed consents.

[23] **Note:** The Center should identify the type of request as well as the individuals or entities (or classes of individuals or entities) to whom the request is routinely made.

[24] **Note:** The Center should describe the reasons why disclosure of the entire medical record is appropriate.

[25] **Note:** The Center should indicate whether there are any conditions or disclosures.

EXHIBIT D

SIENA RESIDENCE

LOG OF NON-ROUTINE OR NON-RECURRING DISCLOSURES OF REQUESTS FOR AN ENTIRE MEDICAL RECORD

Date of Disclosure/Request	Client Information Disclosed or Requested	Persons/Entities Who Received the Disclosure/Request	Justification

EXHIBIT A

MENTAL HEALTH SERVICES

USES OF CLIENT INFORMATION

Class of Employees[26]	Types of Client Information Used[27]	Conditions on Access (If Any)[28]
Director	All client records	
Medical Director	All client records	
Clinic Coordinator	All client records.	
Interns	Client Medical Records	Only clients they are assigned.
Secretary	Client Billing Records	Only clients they are assigned.

[26] **Note:** The Center should specify various classes of employees who require access to client information (e.g., therapists, clerical staff, billing staff, etc.).

[27] **Note:** The Center should list each category of information to which an employee has access (e.g., medical information, billing records, etc.). If an individual requires access to entire medical records, this access must be indicated and a justification should be included.

[28] **Note:** The Center should indicate whether, for a particular individual, there are any conditions on access. For example, billing staff may only have access to client information when they are preparing a bill.

EXHIBIT B

MENTAL HEALTH SERVICES

ROUTINE OR RECURRING DISCLOSURES OF ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Disclosure[29]	Justification[30]	Conditions on Disclosure (If Any)[31]
Disclosures to payors to prove medical necessity for health care claims.	Disclosure of the entire medical record is necessary to substantiate health care claims. The Center is entitled to rely on health plans to request only the minimum amount of client information necessary.	Disclosures of the entire medical record will only be made to payors when payors request disclosure of the entire medical record. Disclosures will not be made if, in the Center's judgment, a request for disclosure is unreasonable.
New York State Office of Mental Health	Disclosure of entire records is necessary for oversight and re-certification.	No conditions.
Medicaid	Disclosure of entire records is necessary to receive payment for services.	Disclosure of entire medical records will only be allowed when request for disclosure is made.
SSI/SSD	Disclosure of entire records is necessary to certify client is disabled and is receiving required services.	Disclosure of entire medical records will only be allowed when request for disclosure is made.

[29] **Note:** The Center should identify the type of disclosure as well as the individuals or entities (or classes of individuals or entities) to whom the disclosure is routinely made.

[30] **Note:** The Center should describe the reasons why disclosure of the entire medical record is appropriate.

[31] **Note:** The Center should indicate whether there are any conditions on disclosures.

EXHIBIT C

MENTAL HEALTH SERVICES

ROUTINE OR RECURRING REQUESTS FOR ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Requests[32]	Justification[33]	Conditions on Disclosure (If Any)[34]
Requests for entire medical records from other providers for payment purposes.	The entire medical record is necessary to substantiate health care claims.	Requests for entire medical records will only be made when the Center's staff makes the determination that the entire medical record is necessary to justify health care claims.
New York State Office of Mental Health	Disclosure of entire records is necessary for oversight and re-certification.	No conditions.
Medicaid	Disclosure of entire records is necessary to substantiate health care claims.	Disclosure of entire medical records will only be allowed when request for disclosure is made.
SSI/SSD	Disclosure of entire records is necessary to certify client is disabled and is receiving required services.	Disclosure of entire medical records will only be allowed when request for disclosure is made.
S.P.O.A./S.P.A.	Medical records regarding appropriate placement.	Disclosure of necessary records after receiving signed consents.
Mental Health Clinics	Medical records regarding treatment progress.	Disclosure of necessary records after receiving signed consents.
School Districts	Medical records regarding treatment progress.	Disclosure of necessary records after receiving signed consents.

[32] **Note:** The Center should identify the type of request as well as the individuals or entities (or classes of individuals or entities) to whom the request is routinely made.

[33] **Note:** The Center should describe the reasons why disclosure of the entire medical record is appropriate.

[34] **Note:** The Center should indicate whether there are any conditions or disclosures.

EXHIBIT D

MENTAL HEALTH SERVICES

LOG OF NON-ROUTINE OR NON-RECURRING DISCLOSURES OF REQUESTS FOR AN ENTIRE MEDICAL RECORD

Date of Disclosure/Request	Client Information Disclosed or Requested	Persons/Entities Who Received the Disclosure/Request	Justification

EXHIBIT A

RESIDENTIAL SERVICES

USES OF CLIENT INFORMATION

Class of Employees[35]	Types of Client Information Used[36]	Conditions on Access (If Any)[37]
Program Director	All client records.	None.
Program Administrator	All client records.	None.
QA Coordinator	All client records.	None.
QA Associate	Client Records related to Residential Habilitation DDP and CHOICES information including TABS #'s, Medicaid and Medicare information	
Support Services Administrator	All client records.	As needed for assigned duties
Healthcare Administrator RN Supervisor Nurse Managers Residential Nurses	All records, except financial.	None.
Behavioral Services Coordinator Behavioral Specialist	All client records.	None.
Residential Coordinator	All client records.	Access to records for consumers in the homes they supervise. Access to other consumers' information for on-call, team meeting and financial benefit resolutions.

[35] **Note:** The Center should specify various classes of employees who require access to client information (e.g., therapists, clerical staff, billing staff, etc.).

[36] **Note:** The Center should list each category of information to which an employee has access (e.g., medical information, billing records, etc.). If an individual requires access to entire medical records, this access must be indicated and a justification should be included.

[37] **Note:** The Center should indicate whether, for a particular individual, there are any conditions on access. For example, billing staff may only have access to client information when they are preparing a bill.

Residence Manager	All client records.	Their site only.
Asst. Manager	All client records.	Their site only. Limited medical, historical, financial and other information.
Senior Counselor	All client records.	Their site only. Limited medical, historical, financial and other information.
Residence Counselor	ISP, IPOP, Res Hab, Medical Information on Consult forms.	Their site only. Limited medical, historical, financial and other information.
Office Manager	None	
Billing and Entitlements Coordinator	Personal Needs Allowance Clothing Allowance Banking Information Burial Account Information	
Residential Facilities Coordinator	None	

Class of Employees	**Types of Client Information Used**	**Conditions on Access (If Any)**
RNs	All client records except financial.	For site they supervise and some other consumers' medical information for on-call purposes
LPNs	All client records except financial.	For their site only.
Administrative Secretary	All client records.	When necessary for operations.
Office Manager	Consumer names, addresses, phone #'s, family contact info. Other consumer information, as need for operations.	When needed for operations.
Secretary of Residential Records	All client records.	When needed for operations.
Secretary	Consumer names, addresses and phone #'s.	When needed for operations.

EXHIBIT B

RESIDENTIAL SERVICES

ROUTINE OR RECURRING DISCLOSURES OF ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Disclosure[38]	Justification[39]	Conditions on Disclosure (If Any)[40]
Disclosures to payors to prove medical necessity for health care claims.	Disclosure of the entire medical record is necessary to substantiate health care claims. The Agency is entitled to rely on health plans to request only the minimum amount of client information necessary.	Disclosures of the entire medical record will only be made to surveyors when surveyors request disclosure of the entire medical record. Disclosures will not be made if, in the Agency's judgment, a request for disclosure is unreasonable.
OPWDD QA Surveyors	QA or investigation purposes. CC is entitled to rely on State officials to request only the minimum amount of client information necessary.	
Commissioner of Quality Care (CQC) Surveyors	QA or investigation purposes. CC is entitled to rely on State officials to request only the minimum amount of client information necessary.	

[38] **Note:** The Center should identify the type of disclosure as well as the individuals or entities (or classes of individuals or entities) to whom the disclosure is routinely made.

[39] **Note:** The Center should describe the reasons why disclosure of the entire medical record is appropriate.

[40] **Note:** The Center should indicate whether there are any conditions on disclosures.

EXHIBIT C

RESIDENTIAL SERVICES

ROUTINE OR RECURRING REQUESTS FOR ENTIRE MEDICAL RECORDS

Type of Routine or Recurring Requests[41]	**Justification**[42]	**Conditions on Disclosure (If Any)**[43]
Request for entire medical record from referring provider.	For a new admission, in order to have complete information to provide quality treatment.	N/A.

[41] **Note:** The Center should identify the type of request as well as the individuals or entities (or classes of individuals or entities) to whom the request is routinely made.

[42] **Note:** The Center should describe the reasons why disclosure of the entire medical record is appropriate.

[43] **Note:** The Center should indicate whether there are any conditions or disclosures.

EXHIBIT D

RESIDENTIAL SERVICES

LOG OF NON-ROUTINE OR NON-RECURRING DISCLOSURES OF REQUESTS FOR AN ENTIRE MEDICAL RECORD

Date of Disclosure/Request	Client Information Disclosed or Requested	Persons/Entities Who Received the Disclosure/Request	Justification

PRIVACY TOOL # 16

CATHOLIC CHARITIES

(the "Agency")

POLICY AND PROCEDURE

SUBJECT:	**USES AND DISCLOSURES OF CLIENT INFORMATION FOR VARIOUS LEGAL, PUBLIC HEALTH, REGULATORY AND EMPLOYMENT PURPOSES**
REFERENCES:	**45 CFR § 164.512**
EFFECTIVE DATE:	**September 22, 2013**
APPROVED BY:	

***Note*: HIV-related information, genetic information, alcohol and/or substance abuse records and mental health records may enjoy additional confidentiality protections under state and federal laws which are not preempted by HIPAA and must be followed. Questions concerning the disclosure of these types of information should be raised with the Privacy Officer.**

A. USES AND DISCLOSURES MADE FOR HEALTH OVERSIGHT ACTIVITIES

1. Uses and Disclosures for Health Oversight Activities**.** The Agency may disclose protected health information ("PHI") to a health oversight agency, (e.g., a Medicare carrier, Medicaid administrator, PRO, etc.) for oversight activities authorized by law, including audits, civil, and criminal investigations or proceedings, inspections, licensure or disciplinary actions.

2. Exceptions**.** Health oversight activities do not include investigations in which the Client is the subject of an investigation that does not arise out of and is not directly related to: (a) the receipt of health care; (b) a claim for public benefits related to health; or (c) qualification for, or receipt of, public benefits or services when a Client's health is integral to the claim. The rules governing disclosures for law enforcement purposes apply when the request is about a Client for other purposes.

Note: If the Agency is unable to determine whether a request for PHI is for a health oversight activity, the Agency should either ask for an explanation of the purpose of the request or consult with legal counsel. In any event, no Agency personnel should make this determination without first consulting the Privacy Officer, Compliance Officer or both, as appropriate.

B. USES AND DISCLOSURES FOR PUBLIC HEALTH OR EMPLOYMENT PURPOSES.

The Agency may disclose PHI:

1. To Prevent or Control Disease. If required by law for preventing or controlling disease, injury, or disability and the conduct of public health surveillance, interventions or investigations).

2. To Report Child Abuse or Neglect. To the New York State Central Registry or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

3. To fulfill requirements of the Food and Drug Administration. For the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such disclosures include, without limitation, disclosures made for the following purposes:

   a) To collect or report adverse events, product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

   b) To track FDA-regulated products;

   c) To enable product recalls, repairs, replacements or lookbacks (including locating and notifying people who have received products subject to recalls, withdrawals or lookbacks); and

   d) To conduct post marketing surveillance.

4. To Notify Persons of Exposure to Communicable Diseases. If the Agency is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

5. To Disclose Proof of Immunization to Schools. If the Agency obtains agreement, which may be oral, from a parent, guardian, or other person acting in loco *parentis* for the Client, or from the individual if he or she is an adult or emancipated minor. The Agency should document any oral consent.

C. USES AND DISCLOSURES FOR EMPLOYMENT PURPOSES.

The Agency can use and disclose information about an individual who is a member of the workforce of the employer, if the following four requirements are met:

1. Agency is Provider. The Agency is a member of the workforce of such employer (e.g., on-site medical clinic), or provides health care to the individual at the request of the employer:

   a) To conduct an evaluation relating to medical surveillance of the workplace; or

   b) To evaluate whether the individual has a work-related illness or injury;

2. PHI is Work-Related. The PHI consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

3. PHI is Required by Law. The employer needs such findings in order to comply with its obligations to report and record occupational injuries and illnesses under Federal laws and related regulations, such as the Occupational Safety and Health Act, or similar state laws, or to carry out responsibilities for workplace medical surveillance; and

4. Written Notice is Posted. The Agency provides written notice to the Client that the foregoing disclosure will be made to the individual's employer:

   a) by giving a copy of the notice to the individual at the time the health care is provided; or

   b) if the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

D. USES AND DISCLOSURES FOR LAW ENFORCEMENT PURPOSES.

1. Disclosures Concerning Victims of Abuse, Neglect or Domestic Violence.

a.) Except for reports of child abuse as described above, Agency may disclose PHI about a Client whom the Agency reasonably believes to be a victim of abuse, neglect, or domestic violence, if the disclosure is to an appropriate government authority provided that the disclosure is either:

1) required by law and complies with and is limited to the relevant requirements of such law;

2) agreed to by the Client; or

3) authorized by statute or regulations, and:

i. the Agency reasonably believes that the disclosure is necessary to prevent serious harm to the Client or other potential victims; or

ii. the Client is unable to agree due to incapacity, and a government authority represents that (a) the PHI sought is not intended to be used against the Client, and (b) an immediate enforcement activity would be materially and adversely affected by waiting until the Client is able to agree to the disclosure.

b.) The Agency must promptly inform the Client that such a report has been or will be made except in circumstances where:

1) the Agency, in the exercise of its professional judgment, believes that informing the Client would put the Client at risk of serious harm; or

2) the Agency would be required to inform a personal representative of the Client, and the Agency reasonably believes that (i) such personal representative is responsible for the abuse, neglect, or other injury; and (ii) informing such person would not be in the best interests of the Client.

2. Disclosures to Law Enforcement Officials for Law Enforcement Purposes.[44]

Disclosures may be made to law enforcement:

Note: PHI should not be disclosed pursuant to this Section without first speaking to the Privacy Officer, Compliance Officer or legal counsel, as appropriate.

a) when required by law, including laws that require the reporting of certain types of wounds or other physical injuries.

[44] Refer to applicable State and Federal law before making disclosures pursuant to this Section. The release of PHI in response to subpoenas that are not accompanied by a court order or Client authorization is limited by State law and privileges (e.g., NY CLPLR 3122 and 4504.). In addition, there are very specific State and/or Federal requirements regarding what must be included in a subpoena for either mental health or substance abuse treatment records. Therefore, staff should not respond to such subpoenas unless authorized by the Privacy Officer.

b) in compliance with and as limited by the requirements of:

1) a court order, a court-ordered warrant or summons issued by a judge; or

2) an administrative request, including a subpoena or summons from an administrative agency, an investigative demand from an authorized body, or similar process authorized under law, provided that all three of the following requirements are met:

i. the PHI sought is relevant and material to a legitimate law enforcement inquiry;

ii. the request is specific and limited in scope to the extent practicable in light of the purpose for which the PHI is sought; and

iii. De-identified information could not reasonably be used

c.) for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, provided that only the following PHI is disclosed[45]:

1) Name and address;

2) Date and place of birth;

3) Social security number;

4) ABO blood type and Rh factor;

5) Type of injury;

6) Date and time of treatment;

7) Date and time of death, if applicable; and

8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence facial hair, scars and tattoos.

d.) Except as otherwise noted herein, in response to a request about a Client who is or is suspected to be a victim of a crime, other than a domestic abuse victim, if:

1) the Client agrees to the disclosure; or

2) the Agency cannot obtain the Client's agreement because of incapacity or other emergency circumstances; and

i. the law enforcement official states: (a) that such PHI is needed to determine whether a person, other than the Client, violated the law, and is not intended to be used against the Client; and (b) immediate law enforcement activity would be materially adversely affected by waiting until the Client-victim gains sufficient capacity to agree; and

ii. disclosure is in the best interest of the victim.

e.) for the purpose of alerting an officer to the death of a Client which the Agency suspects resulted from criminal conduct.

f.) if the Agency believes in good faith that the PHI is evidence of criminal conduct that occurred on the Agency's premises.

g.) if the Agency provides emergency health care, other than an emergency occurring on the premises of the Agency, and disclosure of the PHI is necessary to alert law enforcement to:

1) the commission and nature of a crime;

2) the location of the crime or victims of the crime; and

3) the identity, description and location of the perpetrator of the crime.

3. Identification a Deceased Person or Cause of Death. Limited disclosures may be made to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or the performance of other duties authorized by law. An Agency that performs the duties of a coroner or medical examiner also may use PHI for such purposes.

4. Funeral Arrangements. Limited disclosures, including disclosures prior to the Client's death, may be made to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the deceased person.

5. Disclosures For Purposes of Workers' Compensation. Limited disclosures may be made as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries or illness without regard to fault.

6. To Avert a Serious Threat to Health or Safety. Limited disclosures may be made if consistent with applicable law, and if the Agency believes, in good faith, that the use or disclosure:

a) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and such disclosure is made to a person or persons reasonably able to prevent or lessen the threat; or

b) is necessary for law enforcement authorities to identify or apprehend an individual:

1) who appears from all the circumstances to have escaped from a correctional institution or from lawful custody; or

2) due to a statement made by an individual admitting participation in a violent crime which may have caused serious physical harm to the victim, if such disclosure is limited to the contents of the individual's statement and provides only the PHI that can be disclosed when identifying a victim, as described above.

EXCEPTION: Use or disclosure under this section may NOT be made if the PHI was obtained by the Agency in the course of treating the individual's tendency to engage in the criminal conduct that is the

[45] Except as otherwise permitted, the Center may not disclose any PHI related to an individual's DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissue for purposes of locating or identifying an individual.

subject of the disclosure, or by means of a request by the individual to be treated or referred for treatment, counseling or therapy for such condition.

7. Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes: The Agency may use or disclose PHI to organ procurement organizations for the purpose of facilitating organ, eye or tissue donation or transplantation.

E. DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS.

The release of PHI in response to subpoenas or discovery requests that are not accompanied by a court order or Client authorization is limited by state law and privileges (e.g., NY CLPLR 3122 and 4504.). In addition, there are very specific State and/or Federal requirements regarding what must be included in a subpoena for either mental health or substance abuse treatment records. Therefore, staff should not respond to such subpoenas unless authorized by the Privacy Officer.

F. DISCLOSURES MADE TO VARIOUS GOVERNMENT AGENCIES. The Agency may disclose PHI in the following situations. Because these are not routine occurrences, the Agency's personnel should refer all questions regarding such disclosures to the Privacy Officer.

1. Uses and Disclosures for Military and Veteran Activities. Uses and disclosures may be made concerning individuals who are members of the armed forces or foreign military for activities deemed necessary by appropriate military command or foreign military authorities.

2. Disclosures for National Security and Intelligence Activities: Disclosure may be made to authorized Federal officials for the performance of lawful intelligence, counter-intelligence, and other national security activities authorized by applicable law.

3. Disclosures for Protective Services for the President and Others: Disclosures may be made to authorized federal officials for the provision of protective services to the President or certain other executive persons or to foreign heads of state.

4. Disclosures to Correctional Institutions and in Other Custodial Situations: Disclosure may be made to a correctional institution or a law enforcement official, if the appropriate individual represents that PHI about an inmate or individual in custody is necessary for:

a) the provision of health care to such individuals;

b) the health and safety of such individual or other inmates;

c) the health and safety of the officers or employees of or others at the correctional institution;

d) the health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, Agency, or setting to another;

e) law enforcement on the premises of the correctional institution; and

f) the administration and maintenance of the safety, security, and good order of the correctional institution.

HIPAA PRIVACY TOOL # 17

CATHOLIC CHARITIES

(the "Agency")

POLICY AND PROCEDURE

SUBJECT:	**ACCESS TO CLIENT INFORMATION AND THE RIGHT TO AMEND CLIENT RECORDS**
REFERENCE:	**45 CFR §§ 164.502(g), 164.524 AND 45 CFR §164.526**
EFFECTIVE DATE:	**September 22, 2013**
APPROVED BY:	

Purpose: The Agency is required by law to provide Clients with an opportunity to inspect and obtain copies of their health care information and to request corrections to such health information. This Policy and Procedure sets forth the requirements Clients must satisfy to access and amend their health care information.

I.ACCESS TO CLIENT RECORDS

A. Requirements for Client Access.

1. General Rule. The Agency will provide Clients with an opportunity to inspect and obtain copies of their health information contained in (a) medical and billing records, (b) enrollment, payment, claims adjudication, and case or medical management records maintained by or for a health plan, and (c) any other records used in whole or in part to make decisions about the Client. These records are collectively referred to as "Designated Records."

2. Completion of a Written Request. In order to obtain access to and/or copies of health information, Clients must sign a written request. All written requests for access to and/or copies of Client health information should be appended to the Client's medical record.

3. Response Required Within 30 Days. All Client requests for access to and/or copies of their health information will be received and processed by the Site Coordinator. The Agency will respond to a Client's request and provide the Client with the requested access, within ten (10) days of the Agency's receipt of the request or provide copies or written notice of denial within thirty (30) days of the Agency's receipt of the request.[46]

4. Manner of Access. The Agency will arrange a convenient time for the Client to inspect and/or obtain a copy of his/her health information, subject to payment of a reasonable copying charge (See Section IA6 below). If the records requested are maintained electronically and the Client requests the records electronically, the Agency will provide the Client copies of the records in the electronic form and format requested by the Client, if readily producible. If the electronic form and format requested by the Client is not readily producible, the Agency will offer the Client other electronic formats that are available on the Agency's system.

[46] ***Note*:** NY Public Health Law §18 and NY Mental Hygiene Law §33.16 require the Agency to allow Clients to inspect their medical records within ten (10) days of a request and to provide copies of Client records within a "reasonable time" after the request.

A health care professional at the Agency may request an opportunity to review the health information with the Client, but such review will not be a prerequisite of access.

5. Providing a Written Summary/Explanation. The Agency may provide a Client with a summary of health information in lieu of access to the actual records, if the Client agrees in writing to receive such a summary and pay the fees to be charged for the summary. The Agency also may provide a Client with a written explanation of the health information to which he/she is given access, if the Client agrees in writing to receive such an explanation and pay the fees to be charged for the explanation.

   a) Fees. The Agency will charge the Client a reasonable, cost-based fee for paper or electronic copies of his/her health information. Per NY law, such costs should not exceed $.75 per page for paper format. However, a Client will not be denied access to his/her health information solely because of an inability to pay. The fee may only include the cost of copying (either in paper or electronic media), including the cost of supplies for creating the paper copy or electronic media (cost of compact disc or USB flash drive) and the labor of copying;[47]

   b) Postage, when the Client has requested that a copy of Client information or a summary/explanation be mailed; and

   c) Preparing an explanation or summary of health information, if agreed to by the Client (See Section IA5 above).

B. Denial of Client Access.[48]

Note: Section B lists the grounds for denial of Client access to designated records under the HIPAA privacy regulations, although this list has been tailored to reflect certain provisions of New York law which may apply. In some instances, the grounds for denial under New York law may be different and may supersede HIPAA requirements. In addition, relevant provisions of New York law or HIPAA may change over time. Therefore, if Agency personnel intend to deny a Client access to his/her Client records, they should first consult with the Agency's Privacy Officer and/or a HIPAA attorney.

1. Grounds for Denying Client Access Without Review. The Agency may deny a Client access to his/her Designated Records based on the following grounds, and the Client will not have a right to have the grounds for this denial reviewed.

   a) The information requested is or was compiled in reasonable anticipation of, or for use in, legal or administrative actions or proceedings;

   b) The information requested is maintained by the Agency laboratory and the information is protected from disclosure by applicable federal law;

[47] Per NY law, such costs should not exceed $.75 per page for paper format.

[48] Note: Section B lists the grounds for denial of Client access to designated records under the HIPAA privacy regulations, although this list has been tailored to reflect certain provisions of New York law which may apply. In some instances, the grounds for denial under New York law may be different and may supersede HIPAA requirements. In addition, relevant provisions of New York law or HIPAA may change over time. Therefore, if Agency personnel intend to deny a Client access to his/her Client records, they should first consult with the Agency's Privacy Officer and/or a HIPAA attorney.

c) *The Client is an inmate in a correctional institution, the Agency is acting under the direction of the institution, provided that obtaining a copy of the Client's health information would jeopardize the Client or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate. While the Agency may deny a request for a copy of the Client's health information in the foregoing circumstances, it will not deny a request to review health information;*

d) *The requested health information is or was created or obtained in the course of research that involves treatment. The request may be denied as long as the research is in progress, provided that the Client agreed to the denial of access when he/she consented to participate in the relevant research. Additionally, the Client must be informed that his/her right of access will be reinstated upon completion of the research; or*

e) *The health information requested was obtained from someone other than a health care provider under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source of the information. This exception <u>does</u> <u>not</u> apply to health information obtained from another health care provider.*

2. <u>Reviewable Grounds for the Denial of Access</u>. The Agency may deny a Client's access to their health information under the following circumstances, but the Client will have a right to have this decision reviewed as described below.

a) *If a licensed health care professional has determined, in his/her professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Client or another person; or*

b) *If the health information at issue makes reference to another person and the request to review all or a part of the health information can reasonably be expected to cause substantial and identifiable harm to persons other than the individual which would outweigh the individual's right to access the information.*

c) *If the request is made by the Client's personal representative and, after consideration of all the attendant facts and circumstances, the request to review all or a part of the health information can reasonably be expected to cause substantial and identifiable harm to the Client or persons other than the individual which would outweigh the Client's right to access the information.*

3. <u>Requests By Parent and Guardians</u>.
HIPAA requires that a Covered Entity treat a "personal representative" as the Client for purposes of the privacy regulations. For unemancipated minors, a "personal representative" is a parent or legal guardian who has the authority to act on behalf of the minor in making decisions related to health care, except that a parent or guardian may not access a minor's information in the following circumstances.

a) *The minor consents to a health care service, no other consent to such service is required by law (regardless of whether the consent of another person has also been obtained) and the minor has not requested that such person be treated as a personal representative;*

b) *The minor may lawfully obtain a health care service without the consent of a parent or guardian and the minor, a court, or another person authorized by law consents to such health care service; or*

c) *A parent or guardian assents to an agreement of confidentiality between a covered health care provider and the minor with respect to a health care service.*

Notwithstanding the foregoing sentence, the Agency may disclose or allow access to health information to a parent or guardian, if an applicable provision of state or other law (including case law) permits or requires the disclosure. The Agency may not disclose the health information (or grant access to the health information) to a parent or guardian, if an applicable provision of state or other law (including case law) prohibits the disclosure (or the granting of access).

Note: NY Public Health Law §18 and NY Mental Hygiene Law §33.16 prohibit the access of parents, guardians and legal representatives to a minor's health information when a health care provider determines that access to the health information would have a detrimental effect on either: (a) the provider's professional relationship with the minor; (b) the care and treatment of the minor; or (c) the minor's relationship with his/her parents, guardian or legal representative. Finally, NY Public Health Law §18 and NY Mental Hygiene Law §33.16 allow the Agency to notify a minor Client over the age of twelve (12) years old of a parent, guardian or legal representative's request for health information, and the Agency may (but does not have to) deny the request if the minor Client objects to it.

4. Determinations by Health Care Professional. Finally, it is important to note that, notwithstanding any requirement of HIPAA or any applicable state law, the Agency may not treat a person as a personal representative of an adult or minor Client if: (a) the Agency has a reasonable belief that the Client has been or may be subjected to domestic violence, abuse or neglect by such person, or treating such person as a personal representative could endanger the Client; and (b) the Agency, in the exercise of professional judgment, decides that it is not in the best interest of the Client to treat the person as the Client's personal representative.

Any questions regarding access to health records by personal representatives, parents, guardians or other persons acting *in loco parentis* should be referred to the Agency's Privacy Officer or to the Agency's HIPAA attorney.

5. Extent of Denial. When denying a Client access to his/her health information for any of the reasons described in this Section above, the Agency will, to the extent possible, give the Client access to any other health information requested.

6. Written Notice of Denial. If a Client's request for access to his/her health information is denied, in whole or in part, the Agency will provide the Client with a written denial within ten (10) days of receiving the Client's request. The denial will be in plain language and will describe the reasons for the denial as well as any review rights the Client may have. The written denial also will contain a description of the steps and complaint procedures that the Client may follow to file a complaint with the Agency (including the name and telephone number of the Privacy Officer or his/her designees) and with the U.S. Department of Health and Human Services. Finally, if the Agency does not maintain the health information requested by a Client but knows where the requested information is maintained, the written denial should inform the Client where to direct his/her request. If the Client requests a review of a denial, the Agency will, within ten (10) days of its receipt of the request, transmit the records and necessary information to the designated reviewing party.

7. Review of Denial. When the Agency denies a Client access to health information on grounds subject to review, the Agency will allow the Client to have the denial reviewed by another licensed health care professional designated by the Agency who was not consulted on any of the initial denials of Client access. The Agency will promptly provide the Client with written notice of the determination by the reviewing health professional and that the Agency must abide by the professional's decision. If the Client requests, the Client can appeal a denial of access to health information to a Medical Records Access Review Committee appointed by the U.S. Department of Health and Human Services[49]. Conflicts should be brought to the Privacy Officer's attention.

II. CLIENT'S RIGHT TO REQUEST AMENDMENTS TO HEALTH INFORMATION

A. Written Requests for an Amendment. With certain exceptions, a Client has the right to request an amendment to his/her health information maintained in a Designated Record. The Agency will require that any requests to amend health information be made in writing. All Client requests for amendments to their health information will be received and processed by the Agency's Privacy Officer (or his/her designee).

B. Timely Manner of Responding to Requests for Amendment.

1. 60-Day Rule. The Agency will act on a Client's written amendment request within sixty (60) days of its receipt as described below.

2. Extension Allowed. If the Agency is unable to act on an amendment request within sixty (60) days of its receipt, the Agency may extend the deadline for its response for up to thirty (30) days. To have such an extension, the Agency will, within sixty (60) days of its receipt of the written request, provide the Client with a written statement of the reasons for the delay and the date by which the Agency will complete its processing of the request. The Agency may have only one such extension of time for action on a request for an amendment.

C. Accepting the Amendment. If the Agency decides to accept a requested amendment, in whole or in part, the Agency will make the amendment by identifying the records that are affected by the amendment and then appending the records or otherwise indicating the location of the amendment. The Agency will inform the Client that the amendment has been accepted.

The Agency will obtain the Client's agreement to have the amended health information shared with other persons, when necessary. If the Client's agreement is obtained, the Agency will make reasonable efforts to provide a copy of the amendment within a reasonable time to: (i) persons identified by the Client as having received the health information previously and needing a copy of the amendment; and (ii) persons, including business associates, that the Agency identifies as having the erroneous health information and which may have relied, or could foreseeably rely, on such information to the detriment of the Client. For example, a business associate who uses health information to make decisions about Clients should be informed of relevant amendments to health information.

[49] NY State law also permits review of denials by a clinical records access review committee in accordance with NY Mental Hygiene law §33.16 and/or NY Public Health Law §18 . In the event of a denial of access, NY Mental Hygiene Law §33.16 and/or NY Public Health Law §18 should also be consulted as applicable.

D. Denying an Amendment Request.

1. Grounds for Denial. The Agency may deny a Client's request for an amendment to his/her health information under the following circumstances:

   a) The Agency did not create the health information at issue (i.e., the records were created by another healthcare provider). However, if the Client provides a reasonable basis to believe that the creator of the health information is no longer available to act on the requested amendment, the Agency will address the request as if the Agency created the records;

   b) The requested amendment is to a record which: (i) is not a Designated Record, or (ii) the Client would otherwise not be; and/or allowed access based on this Policy and Procedure.

   c) The Agency determines the health information in question is accurate and complete.

2. Written Denial. If the Agency denies a requested amendment, in whole or in part, the Agency will provide the Client with a written denial within sixty (60) days of its receipt of the Client's amendment request. The written denial must comply with the following:

   a) explain the basis for the denial;

   b) indicate the Client's right to submit a written statement disagreeing with the denial, and explain the process by which the Client may file such a statement. If the Client does submit a statement of disagreement, the Agency will include the statement with the records at issue. This statement of disagreement, or an accurate summary of the statement, will be included with any future disclosures of such records. The Agency may reasonably limit the length of a statement of disagreement, and the Agency may prepare a written rebuttal to a Client's statement of disagreement;

   c) explain that, if the Client does not submit a statement of disagreement, the Client may request that with any future disclosures of the disputed health information, the Client's request for amendment and the denial will be included; and

   d) include a description of the steps the Client may take to complain to the Agency and to the U.S. Department of Health and Human Services.

E. Amendments Made By Other Covered Entities. If the Agency is informed by another covered entity (e.g., another provider or a health plan) of an amendment made by the covered entity to a Client's health information, the Agency will include the amendment in any Designated Records maintained by the Agency for the Client, to the extent applicable. Additionally, all business associates will be requested, upon receipt of a notice of an amendment, to incorporate any necessary amendments to Designated Records maintained by them on the Agency's behalf.

II. Documentation.

The Agency will maintain documentation of compliance with this policy for six (6) years.

HIPAA PRIVACY TOOL #18

CATHOLIC CHARITIES

POLICY & PROCEDURE

SUBJECT: **ACCOUNTING FOR DISCLOSURE OF CLIENT INFORMATION**

REFERENCE: **45 CFR §164.528**

EFFECTIVE DATE: **April 1, 2003**

APPROVED BY:

1. **Purpose**. It is the Agency's policy to safeguard client information and to protect against any unauthorized access to or release of client information. With certain exceptions (See Section 2 below), clients have a right to receive accountings of the disclosures made by the Agency of their protected health information ("PHI"), which includes most identifiable health information related to the health care and payment for health care of a client (including demographic information).[50] This policy describes how the Agency will record certain disclosures of PHI and provide accountings of these disclosures to clients.

2. **Maintaining Records of Disclosures and Providing Accountings**. In accordance with HIPAA's privacy regulations, the Agency will maintain records of certain disclosures made by the Agency of a client's PHI so that the Agency can provide clients with an accounting of these disclosures upon request. HIPAA only grants individuals a *limited* right to receive an accounting of the Agency's disclosures of their PHI, and there are many circumstances in which the Agency is *not* obligated to account for its disclosures. The Agency is ***not*** required to account for the following disclosures of PHI:

   a. Disclosures to carry out treatment, payment and health care operations (See Privacy Tool #7);
   b. Disclosures of PHI to the client;
   c. Disclosures that are incidental to an otherwise permissible or required use or disclosure of PHI (See Privacy Tool # 23);
   d. Disclosures made pursuant to a HIPAA authorization;
   e. Disclosures in the Agency's client directory;
   f. Disclosures to persons involved in the client's care and notices to family members or friends regarding the client's location, general condition and/or death, subject to the requirements of the privacy regulations (See Privacy Tool # 6);
   g. Disclosures for national security or intelligence purposes, subject to applicable HIPAA requirements (See Privacy Tool # 16);

---

[50] "Protected Health Information" means any information, in any form or medium (including oral, written and electronic communication), that: (i) is created by a health care provider, health plan, health care clearinghouse, or an employer; (ii) relates to an individual's physical or mental health, the provision of health care to an individual, or the payment for the provision of health care to an individual; and (iii) identifies, or could be reasonably expected to be used to identify, an individual. Protected Health Information includes everything from a client's name, address and telephone number to the client's clinical or billing records.

h. Disclosures to correctional institutions or law enforcement officials, subject to applicable HIPAA requirements (See Privacy Tool # 16);
i. Disclosures of a limited data set in accordance with applicable HIPAA requirements (See Privacy Tool # 13); and
j. Disclosures made prior to April 14, 2003.

The Agency does not need to account for the disclosures described in the above list of exceptions, and therefore, the Agency does not need to maintain a record of these disclosures. The Agency does need to account for any disclosures of PHI which are not included in the above list of exceptions. Examples of disclosures which the Agency does need to record and account for are: responses to subpoenas and disclosures to government officials (other than those included in the above list of exceptions).

For those disclosures for which the Agency needs to be able to provide an accounting, the Agency will maintain a log which will be affixed to the left side of each client's medical record. The disclosure log attached as Exhibit A will be used to record these disclosures. Upon a client's written request for an accounting, the Agency will provide a copy of the disclosure log which will include disclosures made during the six (6) year period prior to the request.[51] An individual will be provided with an accounting for a shorter time period, if requested. All requests for an accounting of disclosures will be submitted to, and processed by, the Agency's Privacy Officer (or his/her designee).

3. **Temporary Suspension of Rights to an Accounting.** The Agency will suspend an individual's right to an accounting of disclosures to a health oversight agency or law enforcement official for a time specified by the agency or official. However, the suspension will only occur if an agency or official provides a statement to the Agency that an accounting to the individual would be reasonably likely to impede the agency's activities.

If the Agency receives a *written* statement from a health oversight agency or law enforcement official requesting a temporary suspension of the individual's right to receive an accounting of disclosures to the agency or official, the statement must specify the time period during which the suspension is required.

If the Agency only receives an *oral* request from the agency or official requesting a temporary suspension, the Agency must:

a. document the statement, including the identity of the agency or official making the statement;
b. temporarily suspend the individual's right to an accounting of the disclosures subject to the statement; and
c. limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

4. **Contents of an Accounting.**

a. Generally. The Agency will provide individuals with written accountings upon

[51] **Note**: Disclosures made prior to April 14, 2003 do not need to be included in the accounting.

request which include the following information for each disclosure:

i. The date of the disclosure;
ii. The name of the entity or person who received the client's PHI, and if known, the address of such entity or person;
iii. A brief description of the PHI disclosed; and
iv. A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or in lieu of such a statement, the Agency may instead provide a copy of a written request for a disclosure (for disclosures to the Department of Health and Human Services or other regulatory agencies or officials), as applicable.

Accountings will include applicable disclosures made to or by business associates of the Agency.

b. Multiple Disclosures to the Same Person/Family: If, during the period covered by an accounting, the Agency has made multiple disclosures to the same person or entity, then the Agency need only include the following information about these disclosures in an accounting:

i. The required information listed in Section 4(a) above for the *first* disclosure during the accounting period;
ii. The frequency, periodicity, or number of disclosures made during the accounting period; and
iii. The date of the last such disclosure during the accounting period.

Further, if during the accounting period, the Agency has made disclosures of PHI for a particular research purpose[52] for 50 or more individuals, the accounting may, with respect to such disclosures, provide:

i. The name of the protocol or other research activity;
ii. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
iii. A brief description of the type of PHI that was disclosed;
iv. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
v. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
vi. A statement that the PHI of the client may or may not have been disclosed for a particular protocol or other research activity.

Note: If the Agency provides the accounting of research disclosures described above and if it is reasonably likely that the client's PHI was disclosed for a research protocol or activity, the Agency shall, upon request, assist the client in contacting the entity that sponsored the research and the researcher.

---

[52] **Note**: The Agency only needs to account for those disclosures made for research purposes without a client authorization. All disclosures of PHI for research purposes must comply with HIPAA's applicable research rules (See Privacy Tool # 13).

5. **Time Frame for Providing the Accounting**. No later than sixty (60) days after the Agency's receipt of a request for an accounting, the Agency will:

i. provide the individual with the accounting requested; or

ii. provide the individual with a written statement of the reasons why the accounting will not be provided by the sixty (60) day deadline, which statement will advise the individual of the date by which the Agency will provide the accounting. However, the Agency may only delay the time to provide an accounting once. Further, extensions of more than thirty (30) days are not permitted.

6. **Fees for Accountings**. The Agency will provide the first accounting requested by an individual during any twelve (12) month period free of charge. Thereafter, a reasonable, cost-based fee (which includes reasonable retrieval and respond preparation and mailing costs) may be charged for each subsequent request for an accounting made by the same individual [during any given twelve (12) month period]. Before providing subsequent accountings, however, the Agency will inform the individual of the estimated fee in advance and provide the individual with an opportunity to withdraw or modify his/her request for a subsequent accounting in order to avoid or reduce the fee.

7. **Documentation.** When the Agency provides an accounting of disclosures of PHI, the Agency must keep a copy of the written accounting that is provided to the individual pursuant to this policy. In addition, the Agency must keep copies of all information required to be included in accountings so that the Agency may respond to accounting requests by its clients. The foregoing information must be maintained by the Agency for six (6) years.

EXHIBIT A

SAMPLE DISCLOSURE LOG

Client Name: _____

Medical Record No.: _____

Date of the Disclosure	**Name of the Person or Entity Receiving PHI and the Person's or Entity's Address (If Known)**	**Brief Description of the PHI Disclosed**	**Brief Description of the Purpose of the Disclosure**

Note: Disclosures for treatment, payment or health care operations ***do not*** have to be logged.

HIPAA PRIVACY TOOL #19

Catholic Charities
(the "Agency")

POLICY AND PROCEDURE

SUBJECT: **INTERNAL HIPAA COMPLAINTS AND SANCTIONS FOR VIOLATIONS POLICY**

REFERENCES: **45 CFR § 164.530(d) & 164.530(e)**
DHHS Privacy Guidelines, July 6, 2001

EFFECTIVE DATE: **October 1, 2004**

APPROVED BY:

Purpose: The Agency is required by law to have a process in place for individuals to make complaints regarding privacy issues. The Agency must also have a sanctions procedure to address employee and staff violations of the HIPAA privacy regulations and/or the Agency's privacy-related policies and procedures.

1 **Making Complaints Concerning HIPAA Compliance:**

The Agency's Privacy Officer shall receive all complaints (whether written or oral) regarding: (i) the Agency's privacy policies and procedures; (ii) the Agency's compliance with such policies and procedures; and/or (iii) the Agency's compliance with the requirements of HIPAA's privacy regulations. A form which should be used for making written complaints is attached hereto as Exhibit 1. The Agency's privacy notice to clients describes how clients may make a complaint to the Privacy Officer.

After receiving a HIPAA-related complaint, the Privacy Officer will promptly investigate the complaint and will determine whether any employee(s) or business associates of the Agency were involved in possible HIPAA violations.

2 **Mitigation of a HIPAA Violation:**

The Privacy Officer must take appropriate steps to mitigate, to the extent practicable, any known harmful effect resulting from any violation of the HIPAA privacy regulations or the Agency's privacy policies and procedures.

3 **Employee Sanctions For Non-Compliance:**

If the Privacy Officer makes a determination that a violation of the privacy regulations or the Agency's privacy policies and procedures has occurred, the Privacy Officer shall make written findings concerning:

- the nature of the violation(s);
- the identity of any employee(s) or staff member(s) involved; and
- further action, if any, which should be taken, including, but not limited to, sanctions to be applied against any employee(s) or staff member(s) involved in such violation(s).

4 **Process For Issuing Sanctions For a HIPAA Violation:**

A) **Insubstantial Violation:** If the Privacy Officer determines that a privacy violation has occurred, but that such violation was insubstantial or did not result in the release of protected health information, the Privacy Officer may determine that the violation should be addressed through informal means, which may, but are not required to, include:

i) **Meeting:** A meeting between the Privacy Officer (and/or supervisor) and the individual(s) deemed responsible for the violation so that any non-compliant activity may be addressed and a plan may be formulated to ensure compliance in the future;

ii) **Oral Reprimand:** An oral reprimand by the Privacy Officer (and/or supervisor) directed to any or all individual(s) found to be involved in or responsible for the violation, and such reprimand may be noted in each individual's employment file;

iii) **Written Reprimand:** A written reprimand by the Privacy Officer (and/or supervisor) directed to any or all individual(s) found to be involved in or responsible for the violation, and such reprimand shall be included in each individual's employment file; or

iv) **HIPAA Training:** Mandatory enrollment in HIPAA compliance training sponsored by the Agency.

B) **Substantial Violation:** If the Privacy Officer determines that a violation occurred and that such violation was substantial, or that such violation was a repeat offense, the Privacy Officer shall refer the individual(s) deemed responsible to the appropriate disciplinary policy and sanctioning process as follows:

i) **Staff:** Employees shall be referred to the appropriate official responsible for administering the disciplinary process in accordance with the Agency's employee manual.

ii) **Non-Staff:** Independent contractors shall be disciplined or terminated in accordance with their written contracts or Agency policy.

5 **Records:** The Privacy Officer will record each and every privacy-related complaint received, the investigation undertaken, and the disposition, if any, on the HIPAA Complaint Log attached hereto as Exhibit 2. The Privacy Officer will also keep records of any sanctions imposed for a HIPAA violation, including the underlying HIPAA violation, any employee(s) or staff member(s) involved, and any further action taken, including sanctions. Such information shall be recorded on the HIPAA Sanction Log attached hereto as Exhibit 3. Records related to HIPAA complaints and sanctions for privacy violations shall be maintained for at least six years from the date of creation.

6 **Privacy Policy Against Retaliation:**

The Agency will not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against any individual for the exercise by the individual of any right under, or for participation by the individual in any process, established by this policy, including the filing of a HIPAA complaint, participating or assisting in an investigation related to a HIPAA complaint, filing a complaint with the Secretary of the Department of Health and Human Services concerning HIPAA compliance, or opposing any act or practice prohibited by the HIPAA privacy regulations or the Agency's privacy-related policies or procedures. Further, the Agency will not, as a condition of the provision of treatment, require clients to waive their rights under the privacy regulations, including, without limitation, the right to complain to the Secretary of the Department of Health and Human Services or to the Privacy Officer concerning possible HIPAA violations.

EXHIBIT 1

CATHOLIC CHARITIES
OF LONG ISLAN D

COMPLAINT FORM
FOR VIOLATIONS OF HIPAA PRIVACY REGULATIONS
AND THE AGENCY'S RELATED POLICIES AND PROCEDURES

Complainant's Information (Optional): Date: _____

Name_____Position:_____

Program/Department: _____

Address:_____

City:_____State:_____Zip Code:_____Phone No:_____

Nature and Substance of Complaint: (Please specify whether this complaint concerns a failure to follow Agency polices related to the HIPAA privacy regulations, the nature of any unauthorized disclosures or uses of protected information, if any, or any other areas of suspected non-compliance. Also please identify any employee(s), business associate(s) or staff associated with the incident(s) of non-compliance and the extent to which each are involved.)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

EXHIBIT 2

CATHOLIC CHARITIES
OF LONG ISLAND

HIPAA COMPLAINT LOG

Date	Complaint (optional)	Nature of the Complaint	Investigation Undertaken	Disposition (if any)

File: cc-hipaa priv #19

EXHIBIT 3

CATHOLIC CHARITIES OF LONG ISLAND

HIPAA SANCTION LOG
(Sanctions are noted in the Complaint log)

Date	Nature of the HIPAA Violation	Employee(s) or Staff Involved	Sanction

HIPAA PRIVACY TOOL #20

PRIVACY HOTSPOTS

The following are some suggested focus areas for the Agency's privacy assessment:

1 **Physical Surroundings.** The Privacy Regulations do not necessarily require the agency to make structural changes to their facilities to increase the privacy of client communications. However, certain changes may be easily performed such as: (i) adding doors to client treatment rooms; (ii) installing locks on doors to offices where PHI is stored; and (iii) placing client information out of sight in locked cabinets.

You should tour the facility to find vulnerable areas from a privacy perspective. Areas of particular sensitivity include registration areas and unlocked therapists' offices.

2 **Client Conversations.** Since the Privacy Regulations cover oral communications of client information, physicians, therapists and other members of the Agency's workforce should avoid having sensitive conversations with clients in areas where such conversations can be overheard. The Agency may want to add carpeting and/or partitions to reduce noise levels in areas where confidential conversations are frequent. Further, the Agency should consider adopting policies and/or training staff to ensure that client information is reasonably safeguarded during oral communications.[53]

3 **Paper Medical Records.** Access to the areas where client medical records are stored should be limited to staff members with a need for access to these records. The Agency should consider the following suggestions:

- Paper medical records should not be left lying around therapists' unlocked offices, photocopy machines or other areas of the Agency where clients or unauthorized staff members may have access to them;
- Paper medical records should be placed in locked drawers or cabinets; and
- The names of clients on the front of treatment records should not be easily seen by clients in the Agency's waiting area.

4. E-Mail Policies. The Agency should have policies regarding the use of e-mail to send client information. ***All e-mails that are sent outside of the Agency over open networks should be encrypted if they contain client information.*** The Security Guide discusses specific rules and policies regarding the use of e-mail to send client information.

---

[53] Please note, the privacy regulations expressly authorize the incidental uses and disclosures of PHI which occur as a by-product of an otherwise permitted or required use or disclosure. For example, if a therapist discusses a client's case in an office and uses reasonable precautions to prevent others from overhearing, the fact that a person in the hallway overhears the conversation may not be a violation of the Privacy Regulations.

5. **Sign-in Sheets.** While sign-in sheets are useful for the Agency, they may disclose the identity of the Agency's clients. HIPAA does not require the Agency to eliminate sign-in sheets. However, you may want to consider the following suggestions:

- Have a slide-down cover for sign-in sheets which keeps a client that is signing-in from reading the names of other clients on the list;

- Do not list the reason for the visit or the program to be visited on the sign-in sheet; and

- Store the client sign-in sheets behind receptionists' desks and away from the view of clients.

6. **Notification/Follow-up with Clients.** The Agency should be careful when contacting clients at home or at the office, including calls or written reminders to notify clients of upcoming appointments or to follow-up on missed appointments. The Agency should take reasonable steps to ensure that such communications do not disclose client information to unauthorized individuals. For example, the Agency could train its staff to limit the information left on answering machines so that only the minimum necessary amount of information is disclosed (e.g., use a familiar first name and a Agency name that does not reveal the nature of the treatment). The Agency should also avoid disclosing sensitive client information on answering machines or in postcards.

7. **Faxing.** Given the amount of paper that is faxed each day at an average Agency, it is possible that client information may inadvertently be faxed to the wrong number. The Agency can consider the following suggested safeguards:

- Prior to sending a fax, call the recipient to ensure you have the correct number and that the recipient is expecting a fax. The Agency may also want to call recipients to ensure that faxes are received; and

- Avoid locating fax machines in areas in which unauthorized access by clients is possible.

HIPAA PRIVACY TOOL #21

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **BUSINESS ASSOCIATES**

REFERENCES: **45 CFR 164.502(e), 164.504(e)**

EFFECTIVE DATE: **October 1, 2004; September 1, 2024**

APPROVED BY:

POLICY: In accordance with HIPAA regulations, the Agency will obtain and maintain signed Business Associate Addendum Agreements with all Business Associates as defined by HIPAA for all HIPAA covered Programs and/or Departments. The Administrator of each Program or Department is responsible for obtaining a signed Business Associate Addendum from the Business Associates dealing with their program/department. A Business Associate is generally defined as "a person or entity that performs a function or activity on behalf of the covered entity which involves the use or disclosure of Protected Heath Information.

PROCEDURE:
Directors/Administrators are responsible for identifying who is a business associate. They may delegate some of this responsibility to Program Coordinators who have been trained in how to recognize a business associate.

When a business associate is identified, the Director/Administrator reviews the list that is maintained on a Microsoft Word document that is available on our internal support website, Helping Hand.

If no agreement is already in place, the Director/Administrator forwards a Business Associate Addendum with a cover letter explaining the need for the agreement requesting that it be signed and returned to Catholic Charities of Long Island, 90 Cherry Lane, Hicksville, NY 11801 Attn.: Privacy Officer.

Either a Chief Officer or Director may sign the Business Associate Agreement.

It is then returned to the Privacy Officer who copies it and records the name and address of the business associate into a Microsoft Word document that will be available to all on our internal website. The original is maintained by the Privacy Officer. The signed copy is sent back to the Business Associate for their records.

HIPAA BUSINESS ASSOCIATE AGREEMENT / QUALIFIED SERVICE ORGANIZATION AGREEMENT

This Business Associate Agreement, dated as of _____, 202_ ("BA Agreement"), supplements and is made a part of the Services Agreement (as defined below) by and between **Catholic Charities of Long Island** ("Covered Entity") and _____ ("Business Associate"). Covered Entity and Business Associate may be referred to herein collectively as the "Parties" or individually as "Party".

WHEREAS, Covered Entity and Business Associate are parties to the Services Agreement pursuant to which Business Associate provides certain services to Covered Entity. In connection with Business Associate's services, Business Associate creates, receives, maintains or transmits Protected Health Information from or on behalf of Covered Entity, which information is subject to protection under the Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), and related regulations promulgated by the Secretary ("HIPAA Regulations"); and

WHEREAS, Business Associate qualifies as a "business associate" (as defined by the HIPAA Regulations) of its clients, which means that Business Associate has certain responsibilities with respect to the Protected Health Information of its clients; and

WHEREAS, in light of the foregoing and the requirements of HIPAA, the HITECH Act, and HIPAA Regulations, Business Associate and Covered Entity agree to be bound by the following terms and conditions.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Definitions.

    a. General. Terms used, but not otherwise defined, in this BA Agreement shall have the same meaning given to those terms by HIPAA, the HITECH Act and HIPAA Regulations as in effect or as amended from time to time.

    b. Specific.

        i. Breach. "Breach" shall have the same meaning as the term "breach" in 45 CFR § 164.402.

        ii. Electronic Health Record. "Electronic Health Record" shall have the same meaning as the term "electronic health record" in the HITECH Act, Section 13400(5).

        iii. Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to the information that Business Associate creates, receives, maintains, or transmits from or on behalf of Covered Entity.

        iv. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

v. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164.

vi. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

vii. Qualified Service Organization Agreement. "Qualified Service Organization Agreement" shall have the same meaning as defined in 42 CFR 2.12(c)(4).

viii. Required By Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

ix. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

x. Security Rule. "Security Rule" shall mean the Security Standards at 45 CFR Part 160 and Part 164.

xi. Services Agreement. "Services Agreement" shall mean any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to Covered Entity which involve the use or disclosure of Protected Health Information. The Services Agreement is amended by and incorporates the terms of this BA Agreement.

xii. Subcontractor. "Subcontractor" shall have the same meaning as the term "subcontractor" in 45 CFR § 160.103.

xiii. Unsecured Protected Health Information. "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402.

2. Obligations and Activities of Business Associate.

a. Use and Disclosure. Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by the Services Agreement, this BA Agreement or as Required By Law. Business Associate shall comply with the provisions of this BA Agreement relating to privacy and security of Protected Health Information and all present and future provisions of HIPAA, the HITECH Act and HIPAA Regulations that relate to the privacy and security of Protected Health Information and that are applicable to Covered Entity and/or Business Associate. Without limiting the foregoing, to the extent the Business Associate will carry out one or more of the Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

b. Qualified Service Organization. Business Associate acknowledges that it may also be a Qualified Service Organization as defined in 42 CFR 2.11 and as such: (i) acknowledges that, to the extent it receives, stores, processes or otherwise deals with any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug

program, it is fully bound by the regulations in 42 CFR Part 2; and (ii) if necessary, will resist in judicial proceedings any efforts to obtain access to any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program, except as permitted by 42 CFR Part 2.

c. Appropriate Safeguards. Business Associate agrees to use appropriate safeguards and comply, where applicable, with the Security Rule to prevent the use or disclosure of the Protected Health Information other than as provided for by this BA Agreement. Without limiting the generality of the foregoing sentence, Business Associate will:

   i. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information as required by the Security Rule; and

   ii. Ensure that any Subcontractor to whom Business Associate provides Electronic Protected Health Information agrees in writing to implement reasonable and appropriate safeguards and comply, where applicable, with the Security Rule to protect Electronic Protected Health Information and comply with the other requirements of Section 2(a) above.

d. Reporting. Business Associate agrees to promptly, and in any event within three (3) business days, report to Covered Entity any of the following:

   i. Any use or disclosure of Protected Health Information not permitted by this BA Agreement of which Business Associate becomes aware.

   ii. Any Security Incident of which Business Associate becomes aware.

   iii. The discovery of a Breach of Unsecured Protected Health Information.

   A Breach is considered "discovered" as of the first day on which the Breach is known, or reasonably should have been known, to Business Associate or any employee, officer or agent of Business Associate, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include the identification of each Individual whose Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during such Security Incident or Breach as well as any other relevant information regarding the Security Incident or Breach. Any such notice shall be directed to Covered Entity pursuant to the notice provisions of the Services Agreement or to the Privacy Officer of Covered Entity.

e. Investigation. Business Associate shall reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this BA Agreement and/or any Security Incident or Breach.

f. Reports and Notices. Business Associate shall reasonably cooperate and coordinate with Covered Entity in the preparation of any reports or notices to the Individual, a regulatory body or any third party required to be made under HIPAA, HIPAA Regulations, the HITECH Act, or any other Federal or State laws, rules or regulations, provided that any such reports or notices shall be subject to the prior written approval of Covered Entity.

g. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate or its employees, officers, Subcontractors or agents in violation of the requirements of this BA Agreement (including, without limitation, any Security Incident or Breach of Unsecured Protected Health Information). Business Associate shall keep Covered Entity fully apprised of all mitigation efforts of the Business Associate required under this Section 2(g).

h. Subcontractors. Business Associate shall ensure that any Subcontractor to whom Business Associate provides Protected Health Information received from, or created, maintained, received or transmitted by, Business Associate on behalf of Covered Entity agrees in writing to the same restrictions and conditions that apply through this BA Agreement to Business Associate with respect to such information.

i. Access to Designated Record Sets. To the extent that Business Associate possesses or maintains Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of Covered Entity, within three (3) business days of such request, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under HIPAA Regulations. If an Individual makes a request for access to Protected Health Information directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

j. Amendments to Designated Record Sets. To the extent that Business Associate possesses or maintains Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to HIPAA Regulations at the request of Covered Entity or an Individual, within three (3) business days of any such request. If an Individual makes a request for an amendment to Protected Health Information directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

k. Access to Books and Records. Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or to the Secretary, within three (3) business days of such request or in the time and manner otherwise designated by the Secretary or Covered Entity, for purposes of the Secretary or Covered Entity determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

l. Accountings. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with HIPAA, HIPAA Regulations and the HITECH Act.

m. Requests for Accountings. Business Associate agrees to provide to Covered Entity or an Individual, within twenty (20) days of a request by Covered Entity, information collected in accordance with Section 2(l) of this BA Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in

accordance with HIPAA, HIPAA Regulations and the HITECH Act. If an Individual makes a request for an accounting directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

3. Permitted Uses and Disclosures by Business Associate.

   a. Services Agreement. Except as otherwise limited in this BA Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate HIPAA, HIPAA Regulations or the HITECH Act if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

   b. Use for Administration of Business Associate. Except as otherwise limited in this BA Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

   c. Disclosure for Administration of Business Associate. Except as otherwise limited in this BA Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that (i) disclosures are Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Permissible Requests by Covered Entity. Except as set forth in Section 3 of this BA Agreement, Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

5. Term and Termination.

   a. Term. This BA Agreement shall be effective as of the date of this BA Agreement and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created, received or maintained by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

   b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate of the terms of this BA Agreement, Covered Entity shall either:
      i. Provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, Covered Entity shall terminate: (A) this BA Agreement; (B) all of the provisions of the Services Agreement that involve the use or disclosure of Protected Health Information; and (C) such other provisions, if any, of the Services Agreement as Covered Entity designates in its sole discretion; or

ii. Notwithstanding anything contained in the Services Agreement to the contrary, if Business Associate has breached a material term of this BA Agreement and cure is not possible, immediately terminate: (A) this BA Agreement; (B) all of the provisions of the Services Agreement that involve the use or disclosure of Protected Health Information; and (C) such other provisions, if any, of the Services Agreement as Covered Entity designates in its sole discretion.

c. Effect of Termination.

i. Except as provided in Section 5(c)(ii), upon termination of this BA Agreement, for any reason, Business Associate shall either return or destroy, at the discretion of the Covered Entity, all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

ii. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this BA Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. Indemnity. Business Associate agrees to indemnify, defend and hold harmless Covered Entity and its employees, directors/trustees, members, professional staff, representatives and agents (collectively, the "Indemnitees") from and against any and all claims (whether in law or in equity), obligations, actions, causes of action, suits, debts, judgments, losses, fines, penalties, damages, expenses (including attorney's fees), liabilities, lawsuits or costs incurred by the Indemnitees which arise or result from a breach of the terms and conditions of this BA Agreement or a violation of HIPAA, the HITECH Act or HIPAA Regulations by Business Associate or its employees or agents.

7. Compliance with HIPAA Transaction Standards. When providing its services and/or products, Business Associate shall comply with all applicable HIPAA standards and requirements (including, without limitation, those specified in 45 CFR Part 162) with respect to the transmission of health information in electronic form in connection with any transaction for which the Secretary has adopted a standard under HIPAA ("Covered Transactions"). Business Associate will make its services and/or products compliant with HIPAA's standards and requirements no less than thirty (30) days prior to the applicable compliance dates under HIPAA. Business Associate represents and warrants that it is aware of all current HIPAA standards and requirements regarding Covered Transactions, and Business Associate shall comply with any modifications to HIPAA standards and requirements which become effective from time to time. Business Associate agrees that such compliance shall be at its sole cost and expense, which expense shall not be passed on to Covered Entity in any form, including, but not limited to, increased fees. Business Associate shall require all of its agents and Subcontractors (if any) who assist Business Associate in providing its services and/or products to comply with the terms of this Section 7.

8. Miscellaneous.

a. No HIPAA Agency Relationship. It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Covered Entity and Business Associate for purposes of liability under HIPAA, HIPAA Regulations, or the HITECH Act. No terms or conditions contained in this BA Agreement shall be construed to make or render Business Associate an agent of Covered Entity.

b. Regulatory References. A reference in this BA Agreement to a section in HIPAA, HIPAA Regulations, or the HITECH Act means the section as in effect or as amended or modified from time to time, including any corresponding provisions of subsequent superseding laws or regulations.

c. Amendment. The Parties agree to take such action as is necessary to amend the Services Agreement and/or this BA Agreement from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA, the HIPAA Regulations and the HITECH Act.

d. Survival. The rights and obligations of Business Associate under Sections 5(c), 6 and 8 of this BA Agreement shall survive the termination of the Services Agreement and this BA Agreement.

e. Interpretation. Any ambiguity in this BA Agreement shall be resolved to permit Covered Entity to comply with HIPAA, HIPAA Regulations and the HITECH Act.

f. Miscellaneous. The terms of this BA Agreement are hereby incorporated into the Services Agreement. Except as otherwise set forth in Section 8(e) of this BA Agreement, in the event of a conflict between the terms of this BA Agreement and the terms of the Services Agreement, the terms of this BA Agreement shall prevail. Business Associate's obligations hereunder shall not be subject to any limitations of liability or remedies in the Services Agreement. The terms of the Services Agreement which are not modified by this BA Agreement shall remain in full force and effect in accordance with the terms thereof. This BA Agreement shall be governed by, and construed in accordance with, the laws of the state where the Covered Entity is located , exclusive of conflict of law rules. Each Party hereby agrees and consents that any legal action or proceeding with respect to this BA Agreement shall only be brought in the courts of the state where the Covered Entity is located in the county where the Covered Entity is located. The Services Agreement together with this BA Agreement constitutes the entire agreement between the Parties with respect to the subject matter contained herein, and this BA Agreement supersedes and replaces any former business associate agreement or addendum entered into by the Parties. This BA Agreement may be executed in counterparts, each of which when taken together shall constitute one original. Any PDF or facsimile signatures to this BA Agreement shall be deemed original signatures to this BA Agreement. No amendments or modifications to the BA Agreement shall be effective unless agreed upon by both Parties in writing.

IN WITNESS WHEREOF, the Parties have executed this BA Agreement as of the date set forth above.

Catholic Charities of Long Island [BUSINESS ASSOCIATE]

By: _____ By: _____
Name: Name:
Title: Title:

HIPAA PRIVACY TOOL #22

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **MITIGATION**

REFERENCES: **45 CFR 164.530(f)**

EFFECTIVE DATE: **October 1, 2004**

APPROVED BY:

POLICY: The Agency must mitigate, to the extent practicable, any harmful effects made known to the Agency of a use or disclosure of protected health information that is in violation of its policies and procedures or the requirements of HIPAA by either the Agency or a business associate.

PROCEDURE:
Any situation in which protected health information was used or disclosed in violation of either the Agency's policies or HIPAA must be reported immediately to the Privacy Officer (or Security Officer in the Privacy Officer's absence).

The Privacy Officer must then take appropriate steps to mitigate, to the extent practicable, any known harmful effect resulting from any violation of the HIPAA privacy regulations or the Agency's privacy policies and procedures.

HIPAA PRIVACY TOOL #23

CATHOLIC CHARITIES
(The "Agency")

MISCELLANEOUS PRIVACY RULES

1 **Deceased Clients.** The client records of deceased individuals are entitled to the same protections under the Privacy Regulations as the records of live individuals.

2 **Group Health Plans.** If Agency has established an insured or self-insured health plan for their employees, then the plans may be subject to additional HIPAA requirements. Agency with health plans should consult with a HIPAA expert. With certain exceptions, plan sponsors are generally restricted from receiving PHI regarding group health members without making certain required amendments to plan documents. However, the Privacy Regulations expressly permit group health plans to share enrollment and disenrollment information with employers and other plan sponsors without having to amend plan documents.

3 **Organized Healthcare Arrangements.** If the Agency participates in a joint venture or partnership with another provider, it may be considered to be part of an "Organized Healthcare Arrangement" ("OHCA") with the other provider. An OHCA is an organized system of health care or a clinically integrated health care setting in which two or more providers participate (e.g., an admitting relationship between an Agency and a physician). Providers in an OHCA may use a joint privacy notice for that arrangement. Further, a Business Associate Agreement is not required between participating providers in an OHCA. A Covered Entity that participates in an OHCA may disclose client information to another member of the arrangement for any health care operations of the OHCA. The Agency should consult with a HIPAA expert if it has questions regarding an OHCA.

4 **Documentation/Retention of Records.** The Privacy Regulations require that the Agency document its privacy polices and procedures. Written policies and procedures must be retained for six years along with all of the written forms, communications and documents required by the Privacy Regulations (e.g., authorizations, privacy notices, etc.).

5 **DHHS Investigations.** The Agency is required to disclose client information to the Department of Health and Human Services (DHHS) upon request, when DHHS is conducting an investigation or a compliance review pursuant to HIPAA.

6 **Refraining from Intimidating or Retaliatory Acts.** The Agency may not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against clients for the exercise of their rights under the Privacy Regulations. In addition, Agency may not take retaliatory action against an individual for: (1) filing a complaint with DHHS; (2) assisting in an investigation or compliance review by DHHS; or (3) opposing any act or practice which is unlawful under the Privacy Regulations, provided that such individual has a good faith belief that the practice opposed is unlawful and the manner of the opposition is reasonable and does not involve the disclosure of client information in violation of the Privacy Regulations.

7 **Transition.** The Privacy Regulations have a "grandfathering" clause which allows the Agency to rely on existing consents, authorizations and other express legal permissions which may not meet the requirements of the Privacy Regulations, if they were obtained prior to the compliance date for the Privacy Regulations and if certain other conditions are met. A Covered Entity is authorized to use and disclose client information that is created *prior to* April 14, 2003 pursuant to an authorization or other express legal permission obtained from an individual prior to that date, provided that the authorization or other express legal permission specifically permits such use or disclosure. Further, a Covered Entity may use and disclose for research client information

that it created or received either *prior to or after* April 14, 2003, if the Covered Entity obtained one of the following prior to that date: (i) an authorization or other express legal permission from an individual for the use or disclose his/her client information for the research, (ii) an informed consent for the individual to participate in the research, or (iii) a waiver from an IRB for the research. If, after the compliance date, informed consent is later sought from an individual participating in research, an authorization must be obtained from the individual at that time.

8 **Mitigation.** If the Agency knows of a privacy violation by the Agency or a Business Associate, the Agency must take steps to mitigate, to the extent practicable, the harmful effect of the violation. Any steps taken by the Agency to mitigate a violation should be documented in a written or electronic record.

9 **State Law.** In general, HIPAA and the Privacy Regulations preempt any contrary provisions of state law. However, a state law will not be preempted if the law: (a) imposes more stringent requirements than those imposed by HIPAA, or (b) gives greater privacy rights to individuals. There are also other applicable exceptions to the preemption rule. For questions regarding preemption or state law issues, the Agency should consult with a HIPAA expert.

10 **Employment Records.** The Privacy Regulations clarify that employment records held by a Covered Entity in its role as an employer (e.g., sick notes and disability records) are not covered by the Privacy Regulations. However, if a Covered Entity also provides health care services to an employee, the Covered Entity cannot use the client records for employment purposes without a client authorization.

11. **Incidental Uses and Disclosures.** The Privacy Regulations expressly authorize the incidental uses and disclosures of PHI which occur as a by-product of an otherwise permitted or required use or disclosure. For example, if a provider discusses a client's condition in an Agency office and uses reasonable precautions to prevent others from overhearing, the fact that a person in the hallway overhears the conversation may not be a violation of the Privacy Regulations. DHHS has further indicated that sign-in sheets, and calling out names in waiting areas, and discussions of clients in training discussions may also be permissible. However, this rule would only apply to the extent that a Covered Entity has implemented reasonable safeguards and complied with the requirements of the minimum necessary rule. Therefore, a mistaken disclosure of PHI caused by lax safeguards (e.g., calling out sensitive client information in a public area) could still be a violation.

12. **Consents.** The Privacy Regulations give the Agency the option of obtaining consents from its clients to authorize the Agency to use and disclose client information for treatment, payment and health care operations ("HIPAA Consents"). The use of HIPAA Consents by the Agency is strictly voluntary, and the Agency is authorized to use and disclose client information for treatment, payment and health care operations without a HIPAA Consent. Given the potential confusion for clients and Agency staff which may be caused by using voluntary HIPAA Consents, it is not recommended for the Agency to institute a HIPAA Consent procedure. If the Agency chooses to use HIPAA Consents, it needs to be aware that the HIPAA Consent cannot be used in place of HIPAA authorizations when authorizations are required. HIPAA does not specify the form of a HIPAA Consent or the procedures which the Agency may use to obtain HIPAA Consents. Therefore, HIPAA Consent forms and procedures can be designed by the Agency.

Note: It is important to understand that HIPAA Consents are separate and distinct from other types of consents such as consents for treatment or informed consents. The discussion herein does not relate to consents for treatment or informed consents and the Agency should not alter its procedures for obtaining consents for treatment or informed consents on the basis of this discussion. If the Agency has any questions relating to use of HIPAA consents or the difference between HIPAA Consents and other types of consents, it should consult a HIPAA expert.

13. **Coordination of Benefits.** The Privacy Regulations expressly allow a Covered Entity to use and disclose client information as necessary for coordination of benefits, which is considered a payment purpose.

14. **Sales of Business**. The Privacy Regulations expressly permit a Covered Entity to transfer its client records to another entity upon the sale, transfer, merger or consolidation of all or part of the Covered Entity with another entity, provided that the entity receiving the client records is a Covered Entity or will become a Covered Entity as a result of the sale, transfer, merger or consolidation.

HIPAA PRIVACY TOOL #24

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **PROCEDURE TO ACCOMMODATE REASONABLE REQUESTS BY CLIENT TO RECEIVE PERSONAL HEALTH INFORMATION (PHI) BY ALTERNATE MEANS OF COMMUNICATION OR AT ALTERNATE LOCATION**

REFERENCES:

EFFECTIVE DATE: **April 1, 2003**

APPROVED BY:

In an effort to best serve our clients, the Agency will accommodate reasonable requests by clients to receive PHI by alternate means of communication or at alternate locations. All requests must be made in writing to the Program Coordinator. The purpose of this Policy and Procedure is to ensure that the Agency is in compliance with HIPAA's requirements regarding these requests. Our goal is to safeguard the confidentiality and integrity of client information and to protect against the unauthorized access to, or release of such information.

ALTERNATE MEANS OF COMMUNICATION
If a client is to receive PHI in a manner other than face to face, steps need to be taken to insure that confidentiality is maintained or that the risks of disclosure is acceptable to the client.

Alternate means includes the following methods: facsimile transmission, e-mail, professional delivery service or through a personal representative.

The client must be made aware that there are risks associated with alternate means of communication. These risks include the following:

- That privacy cannot be guaranteed when faxing or e-mailing (For additional information related to faxing information, please see the policy entitled*, "Facsimile Transmission of Health Information".)*
- That we have no control of the information if it is delivered by a professional delivery service, and
- That we will require identification from any personal representative who is not known by staff.

Only information requested by the client may be sent.

When communicating through alternate means it is imperative that staff double check that the communication is being sent to the correct address, phone number or e-mail address. Confirmations and receipts should be kept in the client's file.

ALTERNATE LOCATION

At times it may be necessary to deliver PHI to an alternate location. It is imperative that staff safeguard PHI when it is removed from the program office or site by locking the information in the vehicle used for transportation. If it is to be delivered on a day in the future, the information should be brought into the staff's home at night unless there are extenuating circumstances in which the information is not secure in the home. If that is the case, the staff member should alert their supervisor prior to leaving it in the vehicle overnight.

The staff member who delivers the information should get a signature from the person with whom the information is left if it is not the client.

HIPAA PRIVACY TOOL #25

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **PROCEDURE TO SIGN IN VISITORS AND PROVIDE ESCORTS, WHEN APPROPRIATE**

REFERENCES:

EFFECTIVE DATE: **December 9, 2010**

APPROVED BY: **Corporate Compliance Committee**

PURPOSE: To establish procedures to sign in visitors and provide escorts, when appropriate.

PROCEDURE:
Sign in sheets will be with the receptionist at the entrance of all our facilities.

Sign in sheets will be used for all visitors (clients, visitors, vendors, repair people, employees not assigned to site, etc.) However, at some sites all employees may be required to sign as there may be a more restrictive policy in place.

At appropriate sites, the receptionists will ask all visitors entering our facilities to sign in and out at all times. The receptionist will be responsible for keeping the sign-in sheets confidential.

The receptionist will notify the staff member who the visitor is coming to see. The staff member will be responsible for escorting the visitor to the appropriate program or office, as appropriate.

In sites where there is not a receptionist, the site manager will assign the above noted responsibilities.

HIPAA PRIVACY TOOL #26

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **RECORD RETENTION FOR HIPAA DOCUMENTATION**

REFERENCES:

EFFECTIVE DATE:

APPROVED BY:

POLICY: The Agency will maintain all documentation related to HIPAA for at least 6 years in accordance with HIPAA regulations.

PROCEDURE:
Procedure is found in the Site Purchasing Manual – "Facilities and Maintenance" Section under "Record Retention".

HIPAA PRIVACY TOOL #27

CATHOLIC CHARITIES
(the "Agency")

POLICY & PROCEDURE

SUBJECT: **HIPAA TOOL MODIFICATIONS**

REFERENCES: **45 CFR 164.530(i)**

EFFECTIVE DATE: **October 1, 2004**

APPROVED BY:

POLICY: The Agency will modify policies and procedures (Tools) as needed to conform to current laws and regulations and Agency structure.

PROCEDURE:
When the need to modify policies and procedures related to HIPAA is identified, the need is brought to the attention of the Privacy Officer. The Privacy Officer will oversee the changes.

When the new policy and procedure is written, it shall be reviewed by the Privacy and Security Officers and any other concerned party that either of them determine to be appropriate.for the purpose of obtaining possible suggestions and improvements.

When a consensus is obtained, it will be made effective as of a particular date.

The Tools (HIPAA Policies and Procedures will be distributed to those maintaining copies of the HIPAA Compliance Toolkit.

HIPAA PRIVACY TOOL #28

Catholic Charities

POLICY AND PROCEDURE

SUBJECT: TRANSCRIPTION OF HEALTH INFORMATION

REFERENCE: SAFEGUARDS

EFFECTIVE DATE: (Oriinal Date Unknown; Revised September 1, 2024

APPROVED BY:

Policy: The Agency has adopted this policy to protect the security of electronic health information, as well as to meet its duty to protect the confidentiality and integrity of protected health information. All individuals who participate in the processes of dictation, transcription, maintenance, storage and retrieval of transcribed data of the Agency (hereinafter referred to as "Users") must be familiar with this policy.

A. **GENERAL**

1. **Right to Monitor, Audit, Read.** The Agency reserves the right to monitor, audit, and read transcribed documents. If necessary, the Agency may override user passwords in order to monitor the content and usage of the transcription system.

2. **Training and Authorization Required.** A User may use the transcription system only after having completed proper training and having received proper authorization in accordance with Agency Policy. The Director of Information Technology is responsible for such training and authorization.

3. **User's Acknowledgment Required.** A User may use the transcription system only after signing an acknowledgment stating that the User acknowledges and understands: (i) the User's obligation to protect security and maintain confidentiality when using the transcription system; and (ii) that if the User is a Agency employee, the User may face disciplinary action if he/she does not fulfill his/her obligation to protect security and maintain confidentiality when using the transcription system. The Director of InformationTechnology is responsible for obtaining and keeping such written acknowledgment for each User.

4. **Access.** Access to health information, records, tapes, dictation, or a combination thereof is limited to authorized Users on a need-to-know basis.

5. **Dictation and Dictation Playback.** Dictation and dictation playback should be done in a secure environment that protects the information from being overheard by unauthorized persons. Whenever possible, avoid dictating health information into cellular phones, or into telephones located where others can overhear the dictation, or into answering machines.

6. **Shipping of Dictation.** Dictation on audio cassette tapes, CDs, or other voice medium may be shipped only in accordance with Agency policy, and by carriers authorized by the Director of Information Technology.

7. **Electronic Transmission of Transcribed Data.** Transcribed data shall be electronically transmitted only in the manner authorized by the Director of Information Technology.

8. **Log-off Required.** Users must log off computers and dictation equipment when not dictating/transcribing unless using a pause feature that removes the document from view and denies access until the User reactivates it.

9. **Storage and Deletion of Dictation.** Users may store dictation on an audio cassette tape, CD, or any other medium only: (i) for the length of time necessary to transcribe and review the documentation; and (ii) in a manner that protects against unauthorized access. Once the dictation has been transcribed and that transcribed data is received by the Agency, the dictation on the voice file must be deleted or erased in a manner approved by the Director of Information Technology. Tapes may not be reused until they are first erased.

10. **Transcriber's Identification.** Each report shall indicate the individual who has transcribed the data by an identifier assigned by the Agency.

11. **Release of Client Data.** No User may release any client data except to the individual who dictated the data, the Agency, or persons authorized in writing by the Director of Information Technology or Privact Officer.

B. ENFORCEMENT

Supervisors are responsible for enforcing this Policy. Employees who violate this policy are subject to discipline, up to and including termination from employment, in accordance with the Agency's Sanction Policy. Independent contractors are subject to disciplinary action as set forth in their engagement contracts. All suspected violations by employees or outside services should be reported to the Privacy or Securiy Officer.

HIPAA PRIVACY TOOL #29

CATHOLIC CHARITIES
("Covered Entity")

POLICY AND PROCEDURE

SUBJECT:	**Breach Notification (Protected Health Information)**
REFERENCE:	**Health Information Technology for Economic and Clinical Health Act and its implementing regulations (45 CFR 164.400 – 164.414), HIPAA, NY General Business Law 899-aa**
EFFECTIVE DATE:	**September 22, 2013**
APPROVED BY:	

I. POLICY

Catholic Charities (the "Covered Entity") will notify affected individuals and applicable government agencies, as soon as possible, but in no event more than 60 days after the Date of Discovery of a Breach of Unsecured Protected Health Information in accordance with the requirements of the HITECH Act and the NY Breach Notification Law.

II. DEFINITIONS

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy regulations which compromises the security or privacy of PHI.[54] An acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy regulations is presumed to be a Breach unless it is demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PHI outside the Covered Entity holding the information.

Use means the sharing, employment, application, utilization, examination, or analysis of such information within the Covered Entity that maintains the information.

DHHS means the U.S. Department of Health and Human Services.

HIPAA means the federal Health Insurance Portability and Accountability Act of 1996 (42 USC § 201 *et seq*) and its implementing regulations (45 CFR Part 160 and Part 164).

HITECH Act means the federal Health Information Technology for Economic and Clinical Health Act and its implementing regulations (including 45 CFR 164.400 – 164.414).

[54] Note: A Breach does not require notice under the HITECH Act if it involves PHI de-identified in accordance with HIPAA standards or limited data sets when dates of birth and zip codes have been removed.

Protected Health Information ("PHI") is information that:

A. Is created by a health plan, health care provider, health care clearinghouse or an employer;

B. Relates to an individual's physical or mental health, the provision of health care to an individual, or the payment for the provision of health care to an individual; and

C. Identifies, or could be reasonable expected to be used to identify, an individual.

Unsecured Protected Health Information ("Unsecured PHI") means PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of DHHS.

Note: DHHS has stated that encryption of data in accordance with HIPAA requirements and applicable standards of the National Institute of Standards and Technology ("NIST") is an acceptable manner of securing PHI. Furthermore, shredding or destruction of documents and cleaning, purging or destroying electronic media in accordance with NIST standards are also permitted methods of securing PHI. **Redaction or merely password protecting information are not considered to be effective means of securing PHI.**

III. PROCEDURE

A. DISCOVERY OF BREACH

1. ***Reporting Breaches*. All Covered Entity workforce members, agents, independent contractors, and volunteers (collectively the "Covered Entity Staff") must immediately inform the Covered Entity's Privacy Officer of any potential Breach as soon as possible. While investigating any potential Breach, the Privacy Officer shall fill out a Report Form, in the form attached hereto as** Exhibit A**. Business Associates of the Covered Entity shall report all potential Breaches in accordance with their business associate agreements.**

2. ***Date of Discovery*. A Breach is considered to have occurred at the time of the impermissible access, use or disclosure of Unsecured PHI. A Breach is not, however, considered to have been discovered, for the purposes of the HITECH Act, until:**

a. ***the first day the Breach is known to the Covered Entity or Covered Entity Staff; or***

b. ***the first day that the Covered Entity, by exercising reasonable diligence, should have known of the Breach.***

B. INVESTIGATION

1. ***Conduct an Investigation*. After receiving a report of a potential Breach, the Privacy Officer will promptly investigate the circumstances surrounding the potential Breach and will involve the Security Officer and any other Covered Entity representatives necessary to conduct such investigation. During the investigation, the Privacy Officer will, to the extent possible:**

a. ***determine whether there has been an impermissible access, use or disclosure of PHI;***

b. ***determine who impermissibly accessed, used or received PHI and to whom the PHI was potentially disclosed, if applicable;***

c. ***determine whether the PHI involved in the incident was Unsecured PHI (e.g., was it encrypted);***

d. ***identify the type and amount of PHI involved; and***

e. ***determine what steps have been taken (or should be taken) to mitigate risk (e.g., a confidentiality agreement with the person who received the PHI, obtaining the return of the PHI, reporting the incident to the police, etc.).***

2. ***Notification Prior to the Conclusion of the Investigation*. In some situations in which it is apparent that a Breach has occurred, initial individual notifications may need to be sent prior to the completion of the investigation. The Privacy Officer will be responsible for making a determination of the appropriate timing of the notification based on the requirements of the HITECH Act (See Section III(c)(3) below).**

C. DETERMINATION IF A BREACH OCCURRED

1. *Breach Determination*. Whenever a potential Breach is reported, it is presumed that a Breach has occurred, unless it is demonstrated that there is a low probability that the PHI has been compromised. In addition, the State requirements discussed in Exhibit A will be reviewed.

a. *Notification. If it is determined that a Breach has occurred, individuals will be notified as described in Section D; or*

b. *Risk Assessment. If it is determined that a Breach has not occurred because an exception applies or it is determined that there is a low probability that the PHI has been compromised, the Privacy Officer/Security Officer will document a risk assessment which supports the conclusion that notification of individuals was not required. In making such determination, the Privacy Officer/Security Officer will consider the factors listed on the Risk Assessment form attached as Exhibit B.*

2. *Exceptions*. The following do not constitute a Breach that requires notifications to individuals under the HITECH Act:

a. *The unintentional acquisition, access, or use of PHI by an authorized workforce member or another individual acting under the Covered Entity's authority if the acquisition, access, or use was made in good faith, within the scope of such individual's authority, and does not result in further unauthorized use or disclosure.*

b. *The inadvertent disclosure of PHI from one person to another person, if both persons were authorized to access the PHI at the same Covered Entity, organized health care arrangement, or Business Associate, so long as the PHI is not further acquired, accessed, used or disclosed in an unauthorized manner.*

c. *The unauthorized disclosure of PHI when the Covered Entity or Business Associate has a good faith belief that the person to whom disclosure was made would not reasonably have been able to retain the information.*

D. NOTIFICATION OF AFFECTED INDIVIDUALS

1. *Time Frame for Notification*. If it is determined that notification is required, such notification shall be made without unreasonable delay, but in no event more than 60 days from the Date of Discovery of the Breach. The Covered Entity may delay Breach notifications if a delay is requested by a law enforcement official.

a. *If the request is in writing, the delay may be for as long as requested.*

b. *If it is an oral request, the delay may be for up to 30 days unless a further delay is requested in writing. All oral requests shall be documented by the Covered Entity including the name of the official making, and the date of the request.*

2. *Content of the Notification*. The Privacy Officer/Security Officer will be responsible for arranging the preparation of the required notices of Breaches to individuals. Such notifications must be written in plain language, at an appropriate reading level, using clear language and syntax and must include the following information:

a. *A brief description of what happened, including the date of the Breach and Date of Discovery of the Breach, if known;*

b. *A description of the types of Unsecured PHI that were involved in the Breach;*

c. *Any steps individuals should take to protect themselves from potential harm resulting from the Breach;*

d. *A brief description of the Covered Entity's efforts to investigate the Breach, mitigate harm to individuals, and protect against further Breaches; and*

e. *Contact information for individuals to ask questions or learn information about the Breach, which must include a toll-free telephone number, an email address, website, or postal address.*

Note: Notices should not include a listing of the actual PHI that was breached or other sensitive information in the notices themselves, just a general description of the types of PHI involved in the Breach.

3. *General Method of Notification*. Notice to the individuals affected by a Breach must be provided in written form by first-class mail at the last known address of the individual. Written notice may be provided by e-mail only if the individual agrees to receive e-mail notice and has not withdrawn such agreement.

a. *Notice to a minor or an individual who otherwise lacks legal capacity due to a physical or mental condition may be made to the parent or personal representative of the individual.*

b. *If the Covered Entity knows that the individual is deceased and has the address of next of kin or the individual's personal representative, notice must be sent to the next of kin or personal representative, and not to the individual's emergency contact unless the individual's emergency contact is the individual's next of kin or personal representative. The Covered Entity is not required to provide substitute notice to next of kin or a personal representative if the Covered Entity does not have contact information or has out-of-date contact information for the next of kin or personal representative.*

Note: Urgent Notice may be made when the Privacy Officer/Security Officer determines that there is a possibility of imminent misuse of Unsecured PHI. The Privacy Officer/Security Officer, in these cases, may notify affected individuals by telephone, e-mail or other means, as well as by written notice.

4. *Substitute Notice.* Substitute notice to the individuals will be provided if the Covered Entity has insufficient or out-of-date contact information for affected individuals.

a. *If there are fewer than 10 individuals for whom the Covered Entity has insufficient or out-of-date contact information, an alternative form of notice, such as by telephone or e-mail, newspaper or website will be used.*

b. *If there are 10 or more individuals for whom the Covered Entity has insufficient or out-of-date contact information, the Covered Entity will provide the following forms of substitute notice:*

i. Either (A) conspicuous posting for a period of 90 days on the website homepage or by a noticeable and obvious hyperlink to the information; or (B) conspicuous notice in major print or broadcast media in geographic areas where the affected individuals are likely to reside; and

ii. A toll-free phone number, active for 90 days, at which individuals can learn whether their Unsecured PHI was included in the Breach.

E. NOTIFICATIONS TO AUTHORITIES

1. *Annual Notification to Secretary*. The Privacy Officer will maintain documentation of Breaches involving less than 500 individuals. The form attached as Exhibit C may be used for this purpose. The Privacy Officer will submit to the Secretary, on an annual basis, information regarding Breaches that occurred during the preceding year. The Covered Entity will submit this information no later than 60 days after the end of each calendar year in which the Breach is discovered. The information included in the Breach log will include all of the information included in the Breach notices to individuals.

2. *Notification to DHHS and the Media When 500 or More Affected Individuals are Involved*. If the Breach involves 500 or more individuals of a state, notice must be given to the Secretary of DHHS at the same time that notices are given to individuals. Notice must also be provided to prominent media outlets in the State through a press release.

a. *Notification to the media must include the same information included in written notices to individuals.*

b. *Notification to the media will be made without unreasonable delay, and in no case later than 60 calendar days following the Date of Discovery of the Breach.*

F. MITIGATION

The Covered Entity will make reasonable efforts to mitigate the effects of a Breach and to reduce harm to individuals in accordance with its privacy and security policies which may include the following as well as other efforts: providing credit monitoring services to individuals, retraining staff on privacy policies, or implementing new technical or physical safeguards to protect the privacy of PHI.

G. ADDITIONAL REQUIREMENTS

1. *Complaints*. If the Breach resulted from a complaint, such complaint must also be listed on the Covered Entity's complaint log and the applicable Covered Entity's policy regarding responses to complaints will be followed. (See the Agency's policy regarding complaints).

2. *Security Incident*. To the extent that a Breach involves a security incident, the Security Officer should be immediately informed of the security incident and the Covered Entity's policy regarding responses to security incidents will be followed.

3. *Sanctions*. If sanctions against a workforce member result from a Breach, the Covered Entity's policy regarding sanctions/disciplinary actions should be followed, including, as appropriate, a notation on the Covered Entity's HIPAA sanctions log. (See the Agency's policy regarding Sanctions).

4. *Accounting*. If the Breach resulted from a disclosure, such Breach must be listed on the Covered Entity's accounting of disclosures log for each individual affected by the Breach. (See the Agency's policy regarding Accountings of Disclosures).

Exhibit A

ADDITIONAL STATE NOTIFICATION REQUIREMENTS WHEN SOCIAL SECURITY OR FINANCIAL INFORMATION IS INCLUDED

Additional state notification requirements may be required when individuals' social security numbers or other financial information is included about state residents.

IV. NEW YORK REQUIREMENTS

A. DEFINITIONS

N.Y. Breach Notification Law means New York General Business Law § 899-aa.

Private Information means information consisting of an individual's PHI in combination with any one or more of the following data elements about the individual, when either the applicable information is not encrypted or when it is encrypted and the encryption key has also been **compromised:**

1. Social security number;

2. Driver's license number or non-driver identification card number; or

3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Private Information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

Security Breach means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Private Information about New York residents maintained by the Covered Entity. In determining whether information is reasonably believed to have been acquired by an unauthorized person, the Covered Entity may consider the following factors, among others:

1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;

2. indications that the information has been downloaded or copied; or

3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

B. NOTIFICATIONS

1. *Security Breaches*. **If the Breach is also a Security Breach (e.g., Private Information such as social security number was involved) and New York residents are affected, the Covered Entity will also notify the N.Y. Attorney General, the N.Y. Department of State, and the N.Y. State Office of Cyber Security and Critical Infrastructure. If more than 5,000 New York residents are affected, the Covered Entity will notify consumer reporting agencies.**

2. *Notice Contents*. Such notices to these state and consumer agencies must include a copy of the notifications sent to affected individuals, a description of when and how the notifications were sent and the approximate number of affected individuals.

EXHIBIT B

RISK ASSESSMENT FORM

Date: _____

Name: _____

Date of Incident: _____

Date of Discovery of Incident: _____

Brief Description of Incident:

V. The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification.

A. Describe the patient information involved.

B. Were direct patient identifiers of information included? (i.e. names or social security numbers of patients) YES or NO

C. If no direct identifiers of information were provided, is there a likelihood that the PHI involved could be re-identified based on the context and the ability to link the PHI with other available information? YES or NO

D. Is PHI that was involved sensitive in nature? YES or NO **If Yes, please describe in further detail below.**

VI. Unauthorized person who used the PHI or to whom the disclosure was made

A. Who accessed/used the information or to whom was the information disclosed

B. Was the information disclosed to someone with obligations to protect the privacy of the PHI? (e.g. another covered entity, attorney) Please explain. YES OR NO

C. Was the PHI disclosed to someone with a reason to want to misuse the PHI? (e.g. to an employer or family member) Please explain. YES or NO

VII. Was the PHI actually acquired or viewed

Can you demonstrate that PHI was not accessed (i.e. a laptop was stolen but a forensic analysis shows that the PHI was not accessed) Please explain. YES or NO

VIII. Extent to which the risk of the PHI has been mitigated

A. Have you received satisfactory assurances from the person who received the PHI that they destroyed the information and did not share the PHI? Please explain and attach written attestation if available. YES or NO

B. Describe any other mitigating factors:

CONCLUSION (describe why the combination of these factors supports a finding that there was a low probability of compromise):

Exhibit C

Report Form For Potential HIPAA Breaches

Breach Affecting.

___ 500 or more patients

___ Less than 500 patients

Business Associates. If any business associates were involved in the Breach, please provide the following information:

Name of Business Associate: _____

Description of Breach.

Date(s) of Breach: _____

Date(s) of Discovery: _____

Approximate Number of Patients Affected by the Breach: _____

Type of Breach (Check where appropriate)

_____ Theft

_____ Loss

_____ Improper Disposal

Unauthorized Access

_____ Hacking/IT Incident

_____ Other

_____ Unknown

If "Other" is checked, please explain:

Location of Breached Information at the Time of the Breach (Check where appropriate)

_____ Laptop

_____ Desktop Computer

_____ Network Server

_____ E-Mail

_____ Other Portable Electronic Device

_____

_____ Electronic Medical Record

_____ Paper

_____ Oral

_____ Other

If "Other" is checked, please describe the location of the Breached Information below:

Type of Protected Health Information Involved in the Breach (Check where appropriate)

_____ *Demographic/Clinical Information*

- _____ Name
- _____ Address/Zip
- _____ Date of Birth
- _____ Social Security Number
- _____ Driver's License Number
- _____ Other Identifier
- _____ Medical Record Number
- _____ Diagnoses/Conditions
- _____ Medications
- _____ Lab results
- _____ Physician/Operative reports
- _____ Radiology results

_____ *Financial Information*

- _____ Credit Card/Bank Acct #
- _____ Insurance Claims Information
- _____ Other Financial Information

_____ *Other*

If "Other" is checked, please describe the Breached Information in detail below:

Brief Description of the Breach: Please include a description of the Breach, how the Breach occurred, and any additional relevant information regarding the type of Breach, type of media, and type of protected health information involved in the Breach. Also, please identify any employees, agents or contractors associated with the Breach and the extent to which each are involved.:

Safeguards in Place Prior to the Breach

_____ Firewalls

_____ Secure Browser Sessions

_____ Passwords

_____ Encrypted Wireless

_____ Physical Security (security alarm, locked cabinet) Please specify:

_____ Encryption in place

_____ Anti-virus software

_____ Intrusion detection

_____ Biometrics (e.g. eye, thumb print)

_____ Other

If "Other" is checked, please describe the safeguards in detail below:

Actions Taken in Response to the Breach:

_____ Security and/or Privacy Safeguards

_____ Mitigation

_____ Sanctions

_____ Policies and Procedures

_____ Other

If "Other" is checked, please describe the actions taken in response to the Breach in detail below:

HIPAA PRIVACY TOOL # 30

Volunteer Confidentiality Agreement

I understand that during the course of my volunteer services at Catholic Charities, I may be exposed to personal and confidential information related to clients and employees of Catholic Charities. This information is protected under various Federal and New York State Laws such as the Health Insurance and Portability Act of 1996 (HIPAA) and the "Red Flag Rules" of the Federal Trade Commission.

I agree not to disclose or use any information related to Catholic Charities' clients or employees that I may obtain during my volunteer service in accordance with any laws governing such information. I have been provided the opportunity to ask questions regarding my obligations and I understand that to the extent that I violate my obligations under Federal and State Laws, regulations or rules, I will be subject to civil and criminal penalties under the Federal and State Laws, regulations or rules.

Acknowledged and Agreed:

Signature_____

Print Name _____

Job Title: Volunteer

Date _____

PRIVACY TOOL # 31

Catholic Charities (the "Covered Entity")

POLICY AND PROCEDURE

SUBJECT:	**Electronic Transmission, Use of portable devices and Remote Access**
EFFECTIVE DATE:	**April 3, 2025**
APPROVED BY:	**Robert Manfredi**

PURPOSE:
This policy and procedure establishes the security precautions to be used by the employees, interns and volunteers ("Staff") who access or use Covered Entity's electronic systems to transmit, store, disclose, or receive electronic protected health information ("EPHI").

This policy and procedure provides direction to:

- **Staff that send and receive electronic transmissions or use laptop computers and other portable electronic devices (e.g., mobile phones, tablets) to access and send EPHI in order to perform job functions.**
- **Staff that access Covered Entity's information systems remotely from computers located in their homes, remote offices or other locations.**

POLICY:
Staff who send and receive EPHI, using laptops or other portable electronic devices or who access EPHI from external computers are required to take reasonable precautions to protect the confidentiality of EPHI and the devices that store EPHI.

PROCEDURE:

1. Removal of PHI.

a. Staff are not permitted to remove EPHI from Covered Entity unless specifically authorized by their Program Director/Coordinator or the IT Director.

b. In evaluating whether to give authorization for removal of EPHI, Covered Entity will consider the security features of the applicable portable device or mode of transmission (e.g., encryption, password protection, automatic account locking, or secure file transfer).

2. Use of Laptops. Staff must comply with the following requirements:

a. Use of laptops to transmit or receive EPHI must be limited to that which is necessary for Permitted Purposes.

b. When using laptops to transmit, receive or store EPHI, or access the System, implement the following technical safeguards:

i. Ensure laptops are encrypted, unless otherwise authorized.

ii. Ensure laptops have automatic account locking, after no greater than fifteen (15) minutes, requiring entry of a password to re-access the laptop.

iii. Install and enable security software to protect against malicious applications (e.g., viruses, spyware, malware-based attacks) and keep such security patches up-to-date.

iv. Do not plug personal laptops into the Agency network unless approved by the IT Director.

v. Personal laptops are permitted to access the agency wi-fi since it is segregated off from our business network.

3. Use of Tablets and Mobile Phones. Staff must comply with the following requirements:

a. Use of tablets and mobile phones to transmit or receive EPHI must be limited to that which is necessary for Permitted Purposes.

b. When transmitting, receiving or storing EPHI, or accessing the System, implement the following technical safeguards:

i. The tablets and mobile phones must have a screen lock. The user can choose any of the following methods:

1. Pattern (user must draw a pattern out of a grid of dots)

2. PIN (user must enter a numeric code)

3. Password (user must enter an alpha-numeric password)

4. Fingerprint (user must use a biometric unique identifier)

5. Facial Recognition

ii. If a modern device has a screen lock, then it should be automatically encrypted.

iii. Ensure the tablets and mobile phones have automatic account locking, after no greater than fifteen (15) minutes, requiring entry from a lock screen.

iv. Do not jailbreak or root (modify the operating system on) tablets or mobile phones that store, or are used to access, EPHI.

4. Use of portable storage devices (USB flash drives, floppy disks, etc.). Staff must comply with the following requirements:

a. Use of portable storage devices to transmit or receive EPHI must be limited to that which is necessary for Permitted Purposes.

b. When using portable storage devices to transmit, receive or store EPHI, or access the System, Staff may only use encrypted portable storage devices.

5. Email. EPHI may be sent by email in accordance with the following terms of this Policy:

a. No EPHI shall be sent via e-mail to anyone not having an Agency email account (example: user@CatholicCharities.cc)
Exception: An attachment containing EPHI may be sent to any appropriate recipient as long as the files are encrypted.

i. All Microsoft Office files can be manually encrypted by following appropriate steps. Please contact the IT Department for more details.

ii. PDF documents can be encrypted if they are ZIPPed using compression software – with password protection added. Please call the IT Department for more details.

b. In addition, when transmitting EPHI by email, Staff must comply with the following safeguards:

i. Review emails to ensure that they are addressed to the correct recipient.

ii. Include sender contact information on the e-mail.

iii. All emails originating from the Agency automatically contain the approved Catholic Charities signature text which includes our confidentiality statement. Staff should be suspicious if they receive an internal email that does not contain this text.

c. If unusual or unexpected emails are received, verify by telephone that the apparent sender actually sent the email. Contact the IT Department if there is any suspicious activity.

d. Do not forward chain emails or inappropriate emails to the IT Department for analysis.

e. EPHI should only be sent by email for Permitted Purposes.

f. If intending to email service recipients using unencrypted emails, obtain written acknowledgement from the service recipient first regarding the risks of sending email that is unencrypted.

g. If emails contain information that is used to make treatment decisions, the email must be incorporated into the applicable patient's medical record.

h. When available, use Secure File Transfer Protocol (SFTP) to send EPHI as this is the preferred method, particularly for transmission of information pertaining to more than 500 individuals.

i. Whenever mobile phone or tablet utilizes the Agency Corporate Email Server using the Corporate Mail App, the staff must sign and follow the Mobile Device User Access Agreement whether the device is agency owned or staff owned.

j. Use of Outlook on a mobile phone or tablet:
    i. Office 365 policies have been put in place to force the following requirements:

        1. To utilize mobile Outlook, the device must become an Agency managed device. This is true for company owned device, as well as staff personal devices (BYODs).

        2. The only email software application that can be used is the Agency managed mobile Outlook app. Ability to use the native Android and Apple IOS email programs have been blocked.

        3. Only staff that have been approved by the IT Director will be authorized to use mobile Outlook.

    ii. Mobile Outlook data will be deleted remotely from the device if:
        1. The Staff Member's employment terminates.

        2. The Staff Member's job duties change such that mobile Outlook access is no longer appropriate.

        3. The device is reported lost or stolen.

6. Text Messaging. EPHI may be sent by text between Staff members and service recipients, in accordance with the terms of this Policy. Staff sending EPHI by text must comply with the following requirements:

a. Mobile phones used to transmit EPHI by text must comply with the terms of this Policy.

b. Initials or other minimal patient identifiers (e.g., an internally system assigned patient number) rather than patient names must be used, and in general, the amount of EPHI contained in a text should be limited to that information that is absolutely necessary.

c. Particularly sensitive EPHI that is typically subject to additional confidentiality requirements (e.g., information regarding mental health, substance abuse, and HIV treatment) may not be sent by text.

d. Files containing EPHI of more than 500 individuals may not be sent by text.

e. Texts containing EPHI must be deleted as soon as they are addressed.

f. If texting a reminder to a patient, the information in the text should be limited to that information that is absolutely necessary for the patient to understand the nature of the text.

g. Clinic Text Appointment Reminders
    i. The clinics have a method to automatically send text appointments reminders to service recipients who must first sign an authorization form to opt-in to this service.

h. WIC Text Appointment Reminders

    i. The WIC program has the ability to send out text appointment reminders.

7. Use of Virtual Private Network (VPN). Staff must comply with the following requirements:

a. A VPN allows a staff member to temporarily join a remote computer (such as an agency loaner computer) to the Agency network. Once joined, network resources such as shared drives, printers, etc. are available.

b. Use of VPN to transmit or receive EPHI should be limited to that which is necessary for Permitted Purposes.

c. The It Director will grant access to the VPN.

d. The VPN will be secured utilizing a password and Multi Factor Authentication (MFA).

e. When using a VPN to access the System, implement the following technical safeguards on the remote computer:

    i. Install only the approved VPN client software.

    ii. Install and enable security software to protect against malicious applications (e.g., viruses, spyware, malware-based attacks) and keep such security patches up-to-date.

f. When accessing the information remotely, Staff must not leave the applicable computer or portable device unattended while connected to the Covered Entity's computer systems that contain EPHI (the "System").

g. Staff must prohibit unauthorized individuals from using the portable devices or other computers if the Staff Member is connected to the System. Avoid viewing and remotely accessing EPHI in the presence of others (e.g., do not access EPHI while others can "look over your shoulder" to see the EPHI).

h. If a Staff Member's employment terminates or job duties change such that the remote access to EPHI is no longer appropriate, the Staff member's remote access to the System will terminate.

i. Unauthorized individuals are prohibited from using the portable devices if it contains EPHI (e.g., Staff member should not let his or her children use his or her mobile device if the Staff member has EPHI accessible on the mobile device).

j. Report immediately to the Privacy Officer or Security Officer any unauthorized use of, or access to, or loss of, a portable device, computer, or system containing EPHI.

8. Video Streaming/Conferencing.

a. Video streaming/conferencing that may include discussions or images involving EPHI are permissible for Permitted Uses, provided the requirements of this Policy are met.

9. Additional Security Measures

a. Before disposing or reusing portable devices, all PHI stored on them must be deleted/wiped in accordance with the protocols established by Covered Entity.

b. PHI (including EPHI as well as paper) involving more than 20 individuals may not be transmitted through the mail (including UPS, Federal Express, etc.) except on an encrypted portable storage device, unless approved by the Privacy Officer.

c. Report immediately to the Privacy Officer any unauthorized access, use or disclosure of EPHI or violation of this Policy.

10. Risk Assessment.

As part of the periodic security risk assessments performed by the Agency, Catholic Charities will consider the potential risks and vulnerabilities associated with portable devices, remote access and electronic transmission and reevaluate risk management measures to reduce such risks and vulnerabilities to a reasonable and appropriate level.

11. Training

Staff will be trained regarding the vulnerabilities and policies and procedures associated with remote access, portable devices and electronic transmission. Training topics will include:

- Instructions for accessing and transmitting EPHI, password management procedures,
- Rules regarding the downloading of EPHI on portable devices,
- Transmission of EPHI over open networks,
- Dangers of opening attachments from unknown senders, and
- Remote device/media protection.

Such training will also reinforce policies prohibiting the leaving of portable devices and external hardware unattended and potential sanctions for failing to adhere to policies and procedures of portable devices

12. Cloud Based Storage.

a. Cloud Based Storage is the use of a web based service to act as a remote drive (a place to store files and folders).

b. The Agency recognizes the usefulness of cloud based data storage such as Google Drive, Dropbox, Box, or Microsoft One-drive. We also are cognizant of the security risks that are present.

c. Cloud based storage of agency data is permitted as long as no EPHI is stored, and approval is obtained first from the IT Director.

13. Cloud Based Applications.

a. Cloud Based Applications are software programs (examples: Human Resources or Electronic Medical Records) where the software does not reside on a local computer or agency server. The application is installed, maintained, and backed up by an independent software developer.

b. Cloud based applications can contain EPHI, confidential agency data, as well as staff personal data. These applications are permitted to be accessed from any location, even off-site, as long as privacy and security precautions are taken.

14. Enforcement

All Staff are expected to comply with the terms and intent of this Policy. Failure to comply with these terms may result in disciplinary action up to and including termination or termination of access to the System.