Privacy Plan

Version 1.1

Date: 24 April 2024

Revision History

Revision	Revision Date	Owner	Notes
Version 1.0: Privacy Plan	Audit & Compliance Committee approval: 9/30/2022	Deneb Pirrone	Established to replace the Agency Privacy Policy. Board approval required as the Plan replaced a Policy
Version 1.1	4/24/2024	Deneb Pirrone	Security Officer role defined

Table of Contents

Overview…… 3

Part 1: Responsibilities of Catholic Charities as a Covered Entity…… 4

1.1 - Privacy Officer and Security Officer……..... 4
1.2 – Incident Response Team……. 5
1.3 – Staff Member Training…… 5
1.4 – Safeguards……... 5
1.5 – Privacy Notice…… 6
1.6 – Complaints…….. 6
1.7 – Sanctions for Violations of Privacy Plan…… 6
1.8 – Mitigation of Inadvertent Disclosures of Protected Health Information…… 6
1.9 – No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy……. 6
1.10 – Plan Document…….. 7
1.11 – Documentation…….. 7
1.12 – Electronic Health Records……. 8
1.13 – Access Authorization……. 8

Part 2: Use and Disclosure of PHI…… 8

2.1 – Use and Disclosure Defined……. 8
2.2 – Access to PHI Is Limited to Certain Employees……. 9
2.3 – Disclosures of PHI Pursuant to an Authorization…… 9
2.4 – Permissive Disclosures of PHI: for Legal and Public Policy Purposes…….. 10
2.5 – Child Abuse and Reporting Requirement…… 10
2.6 – Judicial Subpoenas……... 11
2.7 – Complying with the "Minimum-Necessary" Standard…… 12
2.8 – Disclosures of PHI to Business Associates……. 13

2.9 – Disclosures of De-Identified Information…… 13
2.10 – Disclosures to Family, Friends or Others-Client Location…… 14
2.11 – Removing PHI from Agency Premises……. 16
2.12 – Faxing PHI…… 16
2.13 – Medical and Social Work Records Governed by Specific Federal and State Statues 17
2.14 – Basic Procedures to Protect Confidential Communications…….. 18

Part 3: Client Individual Rights……. 19

3.1 – Access to Protected Health Information and Requests for Amendment……. 19
3.2 – Accounting……. 19
3.3 – Requests for Alternative Communication Means or Locations……. 20
3.4 – Requests for Restrictions on Uses and Disclosures of Protected Health Information 20
3.5 – When a Client Requests a Copy of his/her/their Record……. 20
3.6 – Client's Request for copy of Clinical Notes or Labs while Checking out After an Appointment……. 20
3.7 – Acceptable Methods of Verification of Identity for Release of Personal Health Information (PHI)……. 21
3.8 – When the requestor is the Clients Legally Authorized Representative……... 21
3.9 – Other Methods……. 21

Part 4: Breach Reporting…….. 22

4.1 – Breach Notification Requirements……..…….. 23
4.2 - Complaint/Concerns Reporting…… 24

Part 5: Legal Counsel Contact…….. 25

Overview

The United States and New York State maintain legislation which provides protection to privileged relationships, insuring that information disclosed within the context of the relationship cannot be disclosed outside the relationship except under certain conditions. For example, the Health Insurance Portability and Accountability Act (HIPAA) and its attendant regulations constrain the abilities of Catholic Charities of Buffalo ("Catholic Charities", 'CCB", "Agency") to use and disclose Protected Health Information (PHI) and the New York State Civil Practice Law & Rules (CPLR) further defines privileged or protected relationships. To codify Agency privacy and security rules pertaining to these regulations, Management has implemented this Privacy Plan ("Plan"), to address privacy and security matters, subject to the Compliance Plan & Code of Ethics policy ("Policy") approved by the Board of Trustees.

What is Protected Health Information?

PHI is any information that is generated, received, or transmitted by the Agency that relates to one of the following:

1. Any past, present, or future physical or mental health condition of a person;
2. Any treatments for said physical or mental health condition(s); or
3. A past, present, or future payment for said treatments.

AND

Identifies the person directly; or a reasonable basis exists to believe the information could be used to identify the person ("Client" for all clients or "Patient" for medical clients only).

Protected health information includes information about persons living or deceased. Examples of PHI include:

- Demographic Information (Address, Telephone Number, etc.)
- Client charts or notes from care providers
- Images of the person
- Medical record numbers or other ID numbers unique to the person
- Computerized records about a person
- Billing information about the person's participation in Agency programs
- Any other health information that can be used to identify an individual or create an inference about the identity of an individual.

What relationships are privileged or protected?

The CPLR defines several privileged relationships that are relevant to CCB. These include Attorney – Client, Physician – Patient, Psychologist – Client, Social Worker – Client, and Rape Crisis Counselor – Client Privilidge, extending to the Agency and staff who have access to Client records. The burden of confidentially exists and commences at intake.

Scope

As Catholic Charities continues to provide services to the community consistent with our mission and core values, it is necessary for CCB to do so in full compliance with HIPAA and other regulatory requirements. As such, all persons who have or gain access to PHI (whether routinely, periodically, or inadvertently) at the Agency must comply with this HIPAA Privacy and Security Plan, which is a set of management protocols and procedures designed to implement the Plan. This includes employees, supervisors, volunteers, interns, vendors, officers, care providers, or anyone whose work performance is under the direct control or responsibility of Catholic Charities, whether paid or unpaid.

The Plan also applies to any person or organization that is NOT a member of Catholic Charities' workforce, acting in a legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services capacity, who has access to individually identifiable health information ("Business Associate(s)").

The term "employee" or "staff member" will henceforth refer to all of these types of workers listed above, including Business Associates.

Some employees or divisions of CCB will be more likely to come into possession of PHI than others; in particular, those working in the following locations or positions (non-exhaustive): Compliance, Clinical Services, other Social Work based programs, Immigration and Refugee Assistance Program, Central Billing, Information Technology, and roles related to providing mental health or counseling services or support.

While the above-mentioned locations, functions, and persons are more likely to come across PHI, **all** employees are required to comply with all HIPAA privacy and information security rules and regulations. If an investigation reveals an employee violated the Plan, the employee will be subject to disciplinary action which could include termination.

PART 1: RESPONSIBILITIES OF CATHOLIC CHARITIES AS A COVERED ENTITY

1.1 - Privacy Officer and Security Officer

The Compliance Officer will be the *ex officio* HIPAA designated **Privacy Officer** for Catholic Charities. The Privacy Officer will be responsible for the development and implementation of initiatives and procedures relating to privacy, including but not limited to this Plan and the Agency's use and disclosure procedures. The Privacy Officer will also serve as the contact person for Clients who have questions, concerns, or complaints about the privacy of their PHI.

The Head of the IT Department will be the *ex officio* HIPAA designated **Security Officer** for Catholic Charities. Per the HIPAA security rule, the Security Officer is responsible for managing information security policies, procedures, and technical systems.

1.2 – Incident Response Team

The Incident Response Team is comprised of the Chief Operating Officer, Chief Financial Officer, and/or additional members deemed appropriate on an *ad hoc* basis in the reasonable judgment of the Privacy Officer. In the event of a security incident results in a wrongful disclosure of PHI, the Privacy Officer, in conjunction with the Incident Response Team and Security Officer will act to prevent further inappropriate disclosures. In addition, Human Resources and legal counsel may be consulted to assist in the investigation of privacy incidents when required. If the Privacy Officer and Incident Response Team are not able to resolve the incident, the Privacy Officer shall involve anyone deemed necessary to secure resolution. If Clients need to be notified of any lost or stolen PHI, the Privacy Officer will send a notice on Agency letterhead to all affected or potentially affected individuals, as required.

1.3 – Staff Member Training

Per Agency's Policy, CCB will train all staff members who have access to PHI on its privacy policies and procedures. All staff members receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is necessary. As circumstances warrant, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Agency's privacy policies and procedures.

1.4 – Safeguards

The Agency has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls and multi-factor authentication. Physical safeguards include locking doors or filing cabinets and periodically changing door access codes. Staff members can only access PHI by using their own login information and are not allowed to share logins with other employees.

Firewalls ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

Data Storage / Backup / Remote Access

Currently all Agency data is backed up using industry standards with off-site storage media. Catholic Charities currently utilizes technology that allows the Security Officer's IT team to quickly start, remove, or disable staff member access to PHI, as needed.

1.5 – Privacy Notice

The Privacy Officer is responsible for developing and maintaining a notice of the Agency's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Agency;
- the individual's rights; and
- the Agency's legal duties with respect to the PHI.

The privacy notice will inform Clients that the Agency will have access to PHI. The privacy notice will also provide a description of the Agency's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all Patients:

- on an ongoing basis, at the time of an individual's enrollment into an Agency program or at the time of treatment and consent; and
- within 60 days after a material change to the notice.

The Agency will also provide notice of availability of the privacy notice at least once every three years.

1.6 – Complaints

The Privacy Officer will be the Agency's contact person for receiving privacy related complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Agency's privacy procedures and for creating a system for handling such complaints. A copy of the complaint form shall be provided to any Client upon request.

1.7 – Sanctions for Violations of Privacy Plan

Sanctions for using or disclosing PHI in violation of this Plan will be imposed in accordance with the Agency's progressive discipline policies up to and including termination.

1.8 – Mitigation of Inadvertent Disclosures of Protected Health Information

Catholic Charities shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of a Client's PHI in violation of the policies and procedures set forth in this Plan. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Agency or an outside consultant/contractor that is not in compliance with this Plan, the employee is required to immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the Client can be taken.

1.9 – No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

Per Policy, no employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating

in an investigation, or opposing any improper practice under HIPAA or any other law, ordinance, ruling, policy/procedure, or regulation.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility.

1.10 – Plan Document

The Plan document includes provisions to describe the permitted and required uses and disclosures of PHI by Catholic Charities. Specifically, the Plan document requires the Agency to:

- Not use or further disclose PHI other than as permitted by the Plan, or as required by law;
- Ensure that any Business Associates, agents, or subcontractors to whom it provides PHI agree to the same restrictions and conditions that apply to Catholic Charities;
- Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- Make PHI available to Clients, consider their amendments, and upon request, provide an accounting of PHI disclosures; and
- Make the Agency's internal practices and records relating to the use and disclosure of PHI received by the Agency available to the Department of Health and Human Services upon request.

1.11 – Documentation

The Agency's privacy policies and procedures shall be documented and maintained for at least seven years. Policies and procedures must be changed as necessary to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy Plan must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

Catholic Charities shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Incident Report

The Agency has developed an Incident Report system. This system is used to document reports of privacy breaches that have been referred to the Management from staff members who have reviewed or received the suspected incident. Incidents involving potential HIPAA violations must be entered into the Incident Report system and escalated to the Privacy Officer.

After receiving the Incident Report form from staff members, the Privacy Officer assesses the incident and its severity and analyzes the situation. Documentation shall be retained by the Agency for a minimum of six years from the date of the reported incident.

If the Privacy Officer is able to resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report System.

1.12 – Electronic Health Records

As with paper records, Electronic Health Records (EHR) must comply with HIPAA, and other state and federal laws. Unlike paper records, electronic health records can be encrypted - using technology that makes them unreadable to anyone other than an authorized user - and security access parameters are set so that only authorized individuals can view them. Further, EHRs offer the added security of an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them.

1.13 – Access Authorization

Catholic Charities will grant access to PHI based on their job functions and responsibilities.

The Privacy Officer, in collaboration with IT and functional Directors, is responsible for the determination of which individuals require access to PHI and what level of access they require through discussions with the individual's supervisor and/or program manager.

The Security Officer will keep a record of authorized users and the rights that they have been granted with respect to PHI. IT keeps a comprehensive matrix of how and to who rights are granted. Due to the nature of many of the Agency's programs, all users of EMR and other case management systems have access to PHI information, with the main limiting designation being to distinguish between Administrators and Users. Administrators have the right to access or remove access to PHI information and Administrator roles are limited to members of the IT department and supervisor level resources in the respective programs.

PART 2: USE AND DISCLOSURE OF PHI

2.1 – Use and Disclosure Defined

The Agency will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

Use – The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Agency, or by a Business Associate of the Agency.

Disclosure – For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable

health information to persons not employed by or working within Catholic Charities with a business need to know PHI.

2.2 – Access to PHI Is Limited to Certain Employees

All staff who performs Client related functions directly on behalf of the Agency or on behalf of group health plans will have access to PHI as determined by their department and job description and as granted by IT.

These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Staff members may not access either through our information systems or the Clients's medical record the medical and/or demographic information for themselves, family members, friends / acquaintances, staff members or other individuals for personal or other non-work related purposes, **even if written or oral Client authorization has been given**. If the staff member is a Client in Catholic Charities plans, the staff member must go through their Provider in order to request their own PHI.

In the very rare circumstance when a staff member's job requires him/her/them to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she/they should immediately report the situation to his/her/their manager who will determine whether to assign a different staff member to complete the task involving the specific Client.

Your access to your own PHI must be based on the same procedures available to other Clients not based on your job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinical note or operative report, you must either contact your physician for the information or make a written request to the Privacy Officer. You cannot access your own information; you must go through all the appropriate channels as any other Client.

2.3 – Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the Client. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

The nature or purpose of "privileged" or "confidential communications" is for the **benefit** and **protection** of the client and places a burden upon the professional to protect and secure the confidentiality of the client's records **until the client should release** the professional from this burden. The client has the right to have access to information about himself/herself contained in

the record subject to Court review (there may be cases where possession of some information could be harmful to the client). In circumstances where the therapist and/or supervisor believe that disclosure of parts or all of the record may be harmful to the client (or somebody who has authority to ask for the record on behalf of the client), the agency has the right to redact that information which may be harmful. The process of redaction **never** happens to the original record.

In the case where the administrative decision is made to deny access to records, in whole or in part, the agency has a duty to notify the client or qualified person of its decision and inform the qualified person of his/her right to obtain a review of the denial free of charge by a committee (Clinical Record Access Review Committee) which is made up of members appointed by the commissioners of OMH, OMRDD, and OASAS. The notice given to the client must explain how the client or qualified person can request a review of the committee.

The agency must send the clinical record to the committee within ten (10) days and explain the specific reasons for denying access to the record or any part thereof. The committee will then review the entire clinical record and offer the client or qualified person the opportunity to be heard. The committee may uphold the denial of access, or may decide to expand access. The determination of the committee is binding on the agency.

2.4 – Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a Client's authorization, when specific requirements are satisfied. The Agency's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

- About victims of abuse, neglect, or domestic violence (including statutory requirement of disclosure to report child abuse as per Section 413 of the New York State Social Services Law);
- For judicial and administrative proceedings (such as Department of Health investigations or audits) or law enforcement purposes;
- For insurance billing and auditing purposes;
- For public health activities;
- For health oversight activities;
- About decedents;
- For cadaver organ, eye, or tissue donation purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers' compensation programs.

2.5 – Child Abuse and Reporting Requirement

A child is a person under 18 years of age (Sec. 1012(e) Family Court Act; Sec. 412 Social Services Law) and is abused when any person **causes**, or any person responsible for a child's

welfare allows infliction of injury (physical or emotional) upon the child or commits, or **allows** to be committed, a sex offense against such child.

In the case of child abuse, a person required to report must:

- Make an oral report, by telephone, immediately to the statewide central register of child abuse and maltreatment (1-800-422-4453) and;
- File a written report within 48 hours of making the required oral report to Child Protection Services, 478 Main Street, Buffalo, New York 14202 (Section 415 Social Services Law) (Exhibit 6 attached).

2.6 – Judicial Subpoenas

The confidentiality of records and the privileged communications contained therein may be challenged by the Judicial subpoena in a Court of Administrative proceedings. A Judicial subpoena is usually issued by an attorney representing a party in an adversary proceeding. The subpoena, in and of itself, **does not** require that the records be produced for examination by the attorney or any person issuing the subpoena or that the person reviewing the subpoena must discuss or disclose any matter in the records prior to the Court proceeding. Judicial subpoenas take two forms.

1. Personal subpoena (**ad testificandum**) directed to an individual demanding that person's attendance at the Court or Administrative hearing in order to take that person's testimony.

2. **Subpoena duces tecum** directing that the records maintained in the ordinary course of business of the Agency pertaining to a case be produced at the Court or Administrative hearing.

Frequently the personal subpoena and the subpoena duces tecum will be combined requiring attendance by the caseworker familiar with the case and producing the records.

The general rule is, that in compliance with the subpoena, the caseworker will attend and/or records will be produced at the Court on the date and time set forth in the subpoena but there will be **no** disclosure of the records or discussion of the case (including discussion in Court waiting or conference rooms) prior to actually appearing in open Court on the witness stand, (there are some exceptions pertaining to County attorneys in parental termination proceedings and Family Court appointed Attorneys for Children given Family Court authorization to case records). In nearly every case where a Court appoints an attorney for a child (AFC), the Court issues, in its Order of Appointment, a directive requiring all treatment providers to communicate with and provide information to the AFC. Where possible, a copy of the Order of Appointment should be obtained from the AFC and kept in the client's file.

The subpoena is a direction to provide testimony or records **in Court** in order to give the Judge the opportunity to rule on whether testimony will be allowed or records received in evidence. In this way a staff caseworker testifying at a trial or proceeding has two natural allies under the law; the defense attorney who has a right to object to testimony being given or records entered into

evidence and the Judge who must render his ruling. Therefore, the caseworker, serving in the capacity as a witness, has no right or need of any additional attorney on his/her behalf. (There could be exceptions e.g. involving protection of the Agency or licensure of the caseworker or situations where it may be necessary for Agency opposition to all or part of the record being disclosed).

Subpoena Service Requirement

A subpoena is legal process and is supposed to be personally delivered to the Agency or an employee. If a subpoenaed witness is required to travel across the jurisdiction of political subdivisions (e.g. Amherst to Buffalo), the subpoena should be accompanied by a mileage check CPLR 8001; $15.00 per day; $.23 per mile round trip). A subpoena for a non-party to an action (or, that third-party's records) is supposed to be served on all parties to that action. **In all cases where a client's records are sought – by someone other than the client who has authorized release), the subpoena MUST be accompanied by a release, authorization or Court Order, or, it is invalid**. In many circumstances, we are presented with subpoena that has been signed by a Judge; in those cases, the Agency has adopted the position that because the Court has the authority to dispense with the confidentiality provisions provided by statute, we accept the Judge's subpoena even if there are technical defects in the instrument or it service.

Pursuant to the provisions of Public Health Law 17 and 18, we are entitled to be reimbursed up to $.75 cents per page for reproducing a record.

It is required that Agency personnel confer with the Agency Attorney, David B. Cotter, before appearing or responding to any subpoena.

2.7 – Complying with the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Department of Labor;
- Uses or disclosures required by law; and
- Uses or disclosure required to comply with HIPAA.

Minimum Necessary When Disclosing PHI – For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed. All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI – For making requests for disclosure of PHI from Business Associates, providers or Clients for purposes of claims payment/adjudication or

internal/external auditing purposes, only the minimum necessary amount of information will be requested. All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

2.8 – Disclosures of PHI to Business Associates

With the approval of the Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the Agency's Business Associates and allow the Agency's Business Associates to create or receive PHI on its behalf. However, prior to doing so, the Agency must first obtain assurances from the Business Associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate agreement ("BAA") is in place.

2.9 – Disclosures of De-Identified Information

The Agency may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

18 specific elements listed below - relating to the Client, employee, relatives, or employer - must be removed, and you must ascertain there is no other available information that could be used alone or in combination to identify an individual.

1. Names;
2. Geographic subdivisions smaller than a state;
3. All elements of dates (but year) related to an individual, to include dates of admission, discharge, birth, death, and the year birth control cannot be used (if px is over 89);
4. Telephone Numbers;
5. Fax Numbers;
6. E-mail addresses;
7. Social Security Numbers;
8. Medical Record Numbers;
9. Health Plan Beneficiary Numbers;
10. Account Numbers;
11. Certificate / License Numbers;
12. Vehicle Identifiers and Serial Numbers (Incl. License Plates);
13. Device Identifiers and Serial Numbers;
14. Web URLs;
15. Internet Protocol Addresses;
16. Biometric Identifiers (Incl. Fingerprints and Voice Prints);
17. Full Face Photos and Similar Images;

18. Any Unique Identifying Number, Characteristic, or Code.

A person with appropriate expertise must determine that 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 the individual. AND this person must document the methods and justification for this determination.

2.10 – Disclosures to Family, Friends or Others-Client Location

There are instances when a Client's friend, acquaintance, or family member contacts Catholic Charities to ask about the location of a Client or whether the Client has been seen at the Agency. Following is guidance provided to assist staff in providing appropriate responses for specific situations that commonly occur. In rare cases of emergency, at the discretion of the Privacy Officer, the minimum of information may be released in order to assist in resolving and emergency situation.

Guidance

Situation: Friends, acquaintances, or family are concerned about the whereabouts of a person. They contact the Agency to ask if a person is at Catholic Charities or has been seen as a Client recently.

Response: If the person is not currently a Catholic Charities Client, the caller may be told that the person is not at the office.

If the person is currently receiving services at the office, office staff should take the name of the caller, their purpose for calling the Client and tell them that they will check. Staff should then ask the Client if it is okay to provide information to the caller and what information to provide. If the Client does not want the office staff to provide information, staff should tell the caller that they are unable to provide information about the Client due to privacy rights and suggest that the caller contact the Client directly for information.

If the caller is asking for historical information about visits or services provided and the Client has not either provided an authorization to share this information with this person pertaining to their involvement in the Client's treatment or payment, the caller should be informed that due to HIPAA confidentiality requirements, information about Client visits is not provided without Client authorization.

Situation: An individual comes to Catholic Charities and tells the reception area that they have arrived to pick up a Client.

Response: If the Client has notified Catholic Charities staff that someone is coming to pick them up (by giving the name of the individual), the individual should be directed to the location of the Client. If the Client has not provided information about anyone coming to pick them up, Catholic Charities staff should ask for the person's name and tell the person that they will check. Another

staff member should be given a note to tell the Client that someone has arrived to pick them up and ask them whether it is okay to tell the person the Client's location.

Additional Guidance for Minors

Generally speaking, minors may only receive medical treatment with the consent of their parents or custodians. In addition, the parent or custodian of a minor, in general, has the authority to consent to the release of information pertaining to the minor.

When minors consent to their own medical treatment, they are entitled to confidentiality of those records; providers may not disclose information about minor – consented treatment to parents or guardians unless they first obtain the minor's consent to do so. All minors may have the right to voice an objection to the disclosure of medical information gathered in the course of their treatment when sharing that information with parents, guardians, or others would pose a threat to the minor's well-being.

Certain categories of minors have a broader right to consent to any and all medical care and therefore to the confidentiality that accompanies consent. Married minors, pregnant minors, and minors who are parents themselves have a statutory right to consent. Emancipated minors have the right to make their own health care decisions without the consent of a parent or guardian.

With regard to minor consent to mental health services, New York Law distinguishes between outpatient and inpatient treatment. Generally, a minor of any age may seek outpatient mental health services without parental involvement if a parent or guardian is not reasonably available, where the provider determines that parental involvement would be detrimental to the course of treatment, or the parent or guardian has refused to give consent and a physician determines that treatment is necessary and in the best interests of the minor [NYMHL §33.21(c); 14 NYCRR §587.7(a)(3)(iii)]. Where parents have refused consent and a physician determines that a minor should receive treatment anyway, the physician must notify the parents of this decision but only if clinically appropriate [NYMHL §3321.21(d)]. A minor must be age 16 or over to consent to inpatient mental treatment [NYMHL §9.13(a)]. If a minor has consented to inpatient treatment, parental consent for medication is not needed. Additionally, a 16 or 17-year-old admitted to inpatient treatment based upon parental consent can give informed consent to medication where medication is in the minor's interests if (1) a parent or guardian is not reasonably available, (2) requiring parental involvement would have a detrimental effect on the minor, or (3) the parent or guardian has refused to consent [NYMHL §33.21(e)(2)].

In court cases involving parents and children, the court will often appoint an attorney for the child (AFC). In nearly every case, whether in fact or in substance, when the court appoints an AFC, it comes with the directive that all treatment providers are required to communicate with and to share information with the AFC. The AFC's duty is to advocate for the child's wishes unless the child to too young to articulate or if the child is making a detrimental choice; in those circumstances, the AFC is required to use his or her best judgment and substitute that judgment for the child's.

The Order of Appointment directing all service providers to communicate and share information with the AFC insulates a social worker from any liability of disclosing any confidential information. You are free to (and required) to communicate with the AFC and provide him or her information about a child you are counseling.

2.11 – Removing PHI from Agency Premises

When Catholic Charities deems it necessary for an employee to work from a location other than one of our sites, PHI may be accessed and/or removed under the following circumstances:

1. Before removing PHI from Catholic Charities for Agency business you must receive the approval from your department Director and IT.
2. Catholic Charities will only allow the paper (Client records, reports) removal of PHI when transported in a secure lock box and when approved by the department Director and the Privacy Officer.
3. Catholic Charities will provide laptop computers for employees required to work offsite and access PHI in a non-Catholic Charities setting. Any files saved on these computers are saved to the network, and are therefore secure.
4. Staff members that work at school sites and create paper files at the school are required to keep these files locked securely. While in transit, these files are kept locked in secured carrying cases.
5. Staff member with progress notes and other forms that need to be signed by their supervisors can be brought back to Catholic Charities in a locked carrying case. These documents can also be saved on the Catholic Charities server in a designated secure file on the Agency network, or on a password-protected flash drive received by IT.
6. The following safeguards are required of all employees when working from a non-Catholic Charities site:
    - When outside the facility, only work on health information in a secure private environment.
    - Keep the information with you at all times while in transit.
    - Do not permit others to have access to the information.
    - Never email Client information.
    - Do not save Client information to your home computer.
    - Do not print records of any type.
    - Do not record login information on or near the computer.
    - Return all information the next business day or as soon as is required.

Catholic Charities will immediately investigate any incident that involves the loss or theft of PHI that was taken off-site.

2.12 – Faxing PHI

Each fax should be accompanied by a Catholic Charities fax cover sheet. Faxing of highly confidential information is not recommended. Faxing of highly confidential information is only permitted if the sender first calls the recipient and confirms that the recipient or his/her/their designee can be waiting at the fax machine, and then, the recipient or his/her/their designee waits

at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of highly confidential information.

If the fax was transmitted to the wrong recipient, in all cases follow these steps:

Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed. Document the incident on an Incident Report Form and notify the HIPAA Privacy Officer at (716) 555-1234. Verify the fax number with the recipient before attempting to fax the information again.

2.13 – Medical and Social Work Records Governed by Specific Federal and State Statues

There are certain records which are governed by specific state and federal statutes and regulations as to disclosure.

Mental Hygiene Records

Section 33.13(a) of the Mental Hygiene Law provides that mental health records maintained at facilities licensed or operated by the Office of Mental health ("OMH"), or the Office Mental Retardation and Developmental Disabilities ("OMRDD"), may not be released to any person or agency outside of the licensed facility without the consent of the patient or someone authorized to act on the patient's behalf. Mental Hygiene Law Section 33.13(e) provides that mental health records maintained at facilities not licensed or operated by OHM or OMRDD may not be released to any person or agency outside of the facility, subject to the same exceptions set forth in subdivisions (b), (c) and (d) of Section 33.13 that also apply to licensed facilities.

Drug and Alcoholism Treatment Records

Records of the identity, diagnosis, prognosis or treatment of any patient that are maintained in connection with the performance of any program or activity relating to alcoholism or alcohol abuse education, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States, are confidential and may only be disclosed for the purpose and under the circumstances expressly authorized by federal statue and regulations.

Records of the identity, diagnosis prognosis, or treatment of any patient that are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States, are confidential and may only be disclosed for the purposes and under the circumstances expressly authorized by federal statute and the regulation (notice must accompany consent form – Exhibit 7 attached).

AIDS or HIV Information

Information concerning whether an individual has been the subject of an HIV related test, or has HIV infection, HIV related illness or AIDS, or information which identifies or reasonably could

identify an individual as having one or more of such conditions, including information pertaining to such individual's contacts, is considered confidential HIV related information pursuant to Article 27-F of the State Public Health Law. No person who obtains confidential HIV related information in the course of providing any health or social services, or pursuant to a release of confidential HIV related information, may disclose or be compelled to disclose such information except under specific circumstances set forth in Public Health law Section 2782. (Exhibits 8a and 8b notice must accompany consent form).

The general consent form for disclosure of confidential information in casework records **cannot** be used for release of HIV related information. Any form of authorization for the release of HIV information must be approved by the Department of Health (N.Y. State Department of Health Form DOH-2557 (65/89) (Exhibit 9 attached) is approved for this purpose). Cases involving Mental Health Records, Drug and Alcoholism Treatment and AIDS or HIV information and release of confidential information pertaining thereto should be handled on a case by case basis after legal consultation.

Privacy Rules for Mental Health and Addiction Crises

In December 2016, the United States enacted the "Helping Families In Mental Health Crisis Reform Act of 2016" which attempts to address the prevention and treatment of mental illnesses and substance abuse, treatment coverage, communication permitted by HIPAA and interactions with law enforcement and the criminal justice system. It changed, to an extent, the use of protected health information to assist an individual (or a family) in crisis, primarily as a result of the opioid epidemic.

2.14 – Basic Procedures to Protect Confidential Communications

1. When authorized to make disclosure, disclose the least amount of confidential information necessary to achieve the desired purpose.

2. Inform clients, to the extent possible, about the disclosure of confidential information and when feasible, before the disclosure is made.

3. When providing counseling services to families, couples, or groups, agreement or understanding should be sought among the parties involved concerning each individual's right to confidentiality and obligation to preserve the confidentiality of information shared by other. However, inform participants in family, couples, or group counseling that there can be no guarantee that all participants will honor such agreement or understanding.

4. Do not discuss confidential information in any setting unless privacy can be assured and avoid discussing confidential information in public or semi-public areas (e.g. hallways, waiting rooms, elevators, and restaurants).

5. Protect the confidentiality of clients' written and electronic records. Take reasonable steps to ensure that clients' records are stored in a secure location and that clients' records are not available to others who are not authorized to have access.

6. Take precautions to ensure and maintain the confidentiality of information transmitted to other parties through the use of computers, electronic mail, facsimile machines, telephone and telephone answering machines, and any other electronic or computer technology. Disclosure of identifying information should be avoided.

7. Do not disclose **identifying** information when discussing clients and/or their records with co-workers for teaching or training purposes or to compare casework strategy on cases, unless the client consents to disclosure of confidential information.

8. Protect the confidentiality of deceased clients consistent with the above and in compliance with New York State statutes regarding social work records.

Part 3: Client Individual Rights

3.1 – Access to Protected Health Information and Requests for Amendment

HIPAA gives Clients the right to access and obtain copies of their PHI that the Agency or its Business Associates maintains. HIPAA also provides that Clients may request to have their PHI amended. The Agency will provide access to PHI and it will consider requests for amendment that are submitted in writing by Clients.

3.2 – Accounting

An individual has the right to obtain an accounting of certain disclosures of his/her/their own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- To carry out treatment, payment or health care operations;
- To individuals about their own PHI;
- Incident to an otherwise permitted use or disclosure or pursuant to an authorization;
- For purposes of creation of a facility directory or to persons involved in the Client's care or other notification purposes;
- As part of a limited data set; or
- For other national security or law enforcement purposes.

The Agency shall respond to an accounting request within 60 days. If the Agency is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the Client notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings. The Privacy Officer is responsible for responding to a request for Accounting.

3.3 – Requests for Alternative Communication Means or Locations

Clients may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, Clients may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of Catholic Charities, the requests are reasonable.

However, Catholic Charities shall accommodate such a request if the Client clearly provides information that the disclosure of all or part of that information could endanger the Client. The Privacy Officer in collaboration with managers has responsibility for administering requests for confidential communications.

3.4 – Requests for Restrictions on Uses and Disclosures of Protected Health Information

A Client may request restrictions on the use and disclosure of the Client's PHI. It is the Agency's protocol to attempt to honor such requests if, in the sole discretion of the Agency, the requests are reasonable. The Privacy Officer is charged with responsibility for processing requests for restrictions.

3.5 – When a Client Requests a Copy of his/her/their Record

A Client can request a copy of his/her/their medical record by completing a Request for Accessing/Inspecting/Copying Health Information form and submitting it to the Department that maintains the information being requested. The Department in collaboration with the Privacy Officer must process and respond to the request. **Note that per management procedures, medical records requested by a Client may not be emailed**.

Clients can receive this form from Client Services or by going directly to the department that maintains their records.

3.6 – Clients Request for copy of Clinical Notes or Labs while Checking out After an Appointment

It is okay to provide a Client with a copy of a clinical note or labs that are maintained in their files. It is recommended that you follow the best practice of stamping or writing "Client Copy" on each page.

3.7 – Acceptable Methods of Verification of Identity for Release of Personal Health Information (PHI)

When the Requestor is the Client

The Agency will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her/their own PHI.

a) **If the request is made in person**, verification of identity may be accomplished by asking for photo identification (such as a driver's license). A copy of the I.D. must be attached to the request and placed in the Clients record.

b) I**f the request is made over the telephone**, verification will be accomplished by requesting identifying information such as social security number, birth date, and medical record number and confirming that this information matches what is in the Client's record. Or, verification will occur through a callback process using phone numbers documented in the Client record to validate the caller's identity.

c) **If the request is made in writing**, verification will be accomplished by requesting a photocopy of photo identification if a photocopy of the ID is not available, the signature on the written request must be compared with the signature in the Client record. In addition, Catholic Charities will need to verify the validity of the written request by contacting the Client by telephone.

3.8 – When the requestor is the Client's Legally Authorized Representative

Verification of identity will be accomplished by asking for a valid photo identification (such as driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record or in the Client's profile as the Client's legally authorized representative. Or, if there is no person listed in the medical record as the Client's legally authorized representative, authority may be established by the person presenting an original of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the Client and a valid photo I.D. A copy of the I.D. and legal notice must be attached to the request and placed in the Clients record.

3.9 – Other Methods

The Agency may use any other method of verification that, in the Agency's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:

- Requesting to see a photo ID
- Requesting a copy of power of attorney or health care proxy documentation
- Confirming personal information with the requestor such as date of birth, policy number or social security number
- Questioning a child's caretaker to establish the relationship with the child

- Calling the requestor back through a main organization switchboard rather than a direct number

PART 4: BREACH REPORTING

The purpose of this section is to address the Agency's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of the Agency. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected e-mails or faxes.

The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Staff members are required to verbally report to his/her/their supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a Client PHI. If the supervisor is unavailable, the staff member must notify the Privacy Officer within 24 hours of the incident. If the supervisor determines that further review is required, the supervisor, staff member, and their senior functional area manager (i.e. Senior Directors in Operations and Directors in other departments, or higher) will consult with the Privacy Officer to determine whether the suspected incident warrants further investigation. In all cases and Incident Report must be submitted to the appropriate reviewer.

The Privacy Officer will document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, or explanation of why corrective actions are not needed, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy breach shall be maintained with the Privacy Officer and shall be retained for at least six years from the date of the investigation. Such documentation is not considered part of the Client's health record.

If the Client is not aware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the Client should be informed. If the Client is aware of a privacy incident, the Privacy Officer shall contact the Client within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer, but resulting communications with the Client must be documented in the incident report. In addition, any privacy incident that includes a disclosure for which an accounting is required must be documented and entered into accounting.

Staff who fail to report known PHI/security incidents, or fail to report them promptly, may be subject to disciplinary action up to termination.

4.1 – Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals if necessary and in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

Media Notice

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

Notice to the Secretary of Health and Human Services

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify

the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a Business Associate, the Business Associate must notify the covered entity following the discovery of the breach. A Business Associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the Business Associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

4.2 – Complaint/Concerns Reporting

Concerns about the Agency's privacy practices may arise in a variety of contexts and may be received by many different persons at the Agency. It is important that the Agency responds to concerns and complaints in a timely manner. When a staff member hears or receives a complaint/concern, he/she/they should ask the complainant whether or not the complainant wishes to file a formal complaint and offer to assist the complainant with the form. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures outlined below.

Filing a Complaint

a) Client's complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a staff member, the person receiving the complaint will:
- In response to a Telephone Call or In-Person Request to File a Complaint – Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Offer to forward a copy of the complaint form to the complainant.
- In response to a Letter or Email (print out) – Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Attach the written complaint to the complaint form.
- In response to an Anonymous Complaint– Complete the Privacy Complaint Form based on the information provided and immediately forward to the Privacy Officer. When possible, explain to the complainant that the Agency has an obligation to follow up on complaints whether or not they are anonymously filed.

b) Staff Members – Call the Privacy Officer at (716) 218-1450 x 2027. Staff members may also complete the Privacy Complaint Form and forward to the Privacy Officer. Staff members can also fill out the complaint form and mail it or put it in the Privacy Officers mail box located at 741 Delaware Avenue, Buffalo, New York 14209. Upon receipt of a complaint, the Privacy Officer will initiate primary investigation.
- *Initial review* – All complaints will be initially reviewed by the Privacy Officer or his/her/their designee to determine if the complaint alleges a violation of

established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her/them of this finding within 60 days. All documentation will be maintained as prescribed in this Plan.

- *Complaints requiring further review* – If there is a legitimate allegation, the Privacy Officer or his/her/their designee will conduct a detailed investigation by reviewing the covered Agency unit practices, contacting employees, Clients, or volunteers as needed, working with the Management team (as applicable), and utilizing other Agency resources as needed. Upon conclusion of the investigation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her/them of the finding within 60 days.

c) 60-day time frame – In the event that this 60-day period cannot be met, the Privacy Officer shall, when possible, communicate this determination to the Complainant in writing and include an estimated timeframe for completion of the investigation.

PART 5: LEGAL COUNSEL CONTACT

Legal question should be directed to David B. Cotter, Attorney, 380 Cleveland Drive, Buffalo, New York 14215. Phone: 716-634-7920, Fax: 716-634-5362, or Email: dbacotter@aol.com.