Arc GLOW

Topic: Health Insurance Portability and Accountability Act (HIPAA)/ Privacy Compliance Plan	**Ref. No**. 345 (A – P)
Department: Corporate Compliance	**Page:** 1 -76
Function: Confidentiality /Privacy	**Originated:** 12/10, 1/22 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020. 3/23/2022, 6/28/2023	**Revised:** 1/2014 – 5/2014, 4/2015, 5/2016, 1/2022
Responsible Director: Compliance Director	**Reviewed:** 11/11, 11/12, 4/2017, 4/2018, 10/2019, 6/2023

ARC GLOW'S
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
PRIVACY COMPLIANCE PLAN

TABLE OF CONTENTS

INTRODUCTION

Arc GLOW (The Arc) strives at all times to maintain the highest degree of integrity in its interactions with the people we support, and the delivery of services. Arc GLOW also strives to maintain compliance with all laws, rules, regulations, and requirements (details can be found at https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)

This Health Insurance Portability and Accountability Act (HIPAA) Privacy Compliance Plan contains Arc GLOW's policies, procedures, and standards of conduct designed to ensure compliance with applicable federal laws and regulations as they apply to HIPAA.

Failure to abide by the rules, policies, and procedures established by this plan, or behavior in violation of any HIPAA law, regulation, or rule may result in disciplinary action. Willful failure to comply with the policies and procedures contained in this plan may result in employment dismissal.

Questions

If you have questions about this HIPAA Compliance Plan, please contact your department's management team, or the agency's Privacy Officer immediately, at 658-2828. It is important that all questions be resolved as soon as possible to ensure protected health information is used and disclosed appropriately.

PRIVACY OFFICER

Arc GLOW's Director of HIPAA and Quality Improvement serves as the agency's Privacy Officer. The Privacy Officer's role is to oversee the development, implementation and maintenance of, and adherence to the organization's policies, procedures, and systems for protecting the privacy of and access to protected health information maintained by the Arc that has the potential to reveal the identity of the people we support. The Privacy Officer is charged with the following responsibilities:

- Oversee and monitor implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Compliance Plan in accordance with applicable federal and state laws

- Ensure that The Arc's Notice of Privacy Practices is current, comprehensive and readily accessible to people supported, their families, guardians, advocates and correspondents, and agency employees

- Serve as a member of the Compliance Committee and report regularly regarding HIPAA privacy and related activity. Assist Compliance Committee Chairperson with reports to the Board of Directors

- Ensure that Business Associate Agreements include required HIPAA language

- Develop and implement a training program and ensure that training materials are appropriate for all Arc GLOW personnel affected by this policy

- Monitor the dissemination of information to independent contractors, as appropriate, informing them of the privacy requirements of the HIPAA Privacy Compliance Plan

- Coordinate the privacy compliance efforts within Arc GLOW, and establish methods to reduce vulnerability to privacy policy abuse

- Review and revise the HIPAA Privacy Compliance Plan on an as needed basis

- Maintain mechanisms to receive and investigate reports of concerns regarding HIPAA privacy abuse or witnessed / reported breaches of privacy policies, standards or procedures, and monitor subsequent corrective action and compliance

- Ensure required breach notifications in accordance with applicable state and federal regulations

The Privacy Officer can be reached by calling 585-658-2828.

TRAINING AND EDUCATION

Arc GLOW employees, Board members, and volunteers are required to receive training on the Health Insurance Portability and Accountability Act (HIPAA) and how the performance of their duties relates to the privacy standards and applicable regulations.

As a result of HIPAA training, each person affected by this policy will understand that complying with the organization's HIPAA policies is a condition of continued employment, contract, or volunteer services.

The initial employee training will be assigned within one month of hire for employees. Employees will receive additional training specific to their responsibilities and the relationship between their duties and the privacy laws during site specific orientation. HIPAA refresher training will be included with

annual Compliance training, and the Privacy Officer/designee will send periodic reminders to all employees regarding standards and / or procedures, based on observations of practices, privacy compliance investigations, or audits.

Board Members and other volunteers will receive training on confidentiality and HIPAA prior to commencing their service.

Attendance at HIPAA privacy training will be documented and recorded on the employee or volunteer's training record either in paper or electronic form. Effective January 1, 2014, documentation of Board Member training will be maintained by the Compliance Officer / designee.

VIOLATIONS

The agency's Privacy Officer has general responsibility for implementation of this plan. Members of our agency workforce who violate this policy will be subject to disciplinary action up to and including termination of employment, service, or contract with Arc GLOW. Anyone who knows or has reason to believe that another person has violated any policy contained herein should report the matter promptly to his/her Supervisor, Program Director, Vice President, or the agency's Privacy Officer.

All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, Arc GLOW will make every effort to handle the reported matter confidentially.

Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment, service, or contract with Arc GLOW.

Arc GLOW

Topic: Notice of Privacy Practices	**Ref. No.** 345- A
Department: Corporate Compliance	**Page:** 1 of 2
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2018, 1/22/2020, 3/23/22	**Revised:** 1/2014, 4/2015, 4/2018, 1/2022, 6/2023
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 5/2016, 4/2017, 4/2018, 10/2019

PURPOSE

The Health Insurance Portability and Accountability Act Privacy Regulations require that Arc GLOW distributes to every person supported a copy of our Notice of Privacy Practices and that the organization makes a good faith effort to obtain from the person supported a written acknowledgement that they have received a copy of such notice. After April 15, 2003, the Notice of Privacy Practices is to be distributed to the person supported the first time we provide services to the person

POLICY

Arc GLOW (Arc) is committed to protecting the privacy of the people we support. Sharing information about a person is only done with those who need to know and who are permitted by law to receive the information. We are required by both federal and state law to protect the privacy and confidentiality of protected health information that may reveal the person's identity.

Arc GLOW will provide to each person supported an Arc GLOW **Notice of Privacy Practices** in accordance with the Health Insurance Portability and Accountability Act. The notice describes how protected health information about the person supported by Arc GLOW may be used and disclosed; how the person supported (individual), his/her legal guardian(s), and/or his/her personal representative can gain access to the information; and the rights of the person supported regarding their protected health information.

POSITIONS PRIMARILY AFFECTED

This policy contains general information that applies to all employees, trainees, Board Members, volunteers, consultants, contractors, and subcontractors of the agency. All must understand and comply with the rights of people supported with

respect to protected health information, in order to assist them with understanding how to exercise those rights. To this end, a copy of Arc GLOW's Notice of Privacy Practices is distributed with training materials.

PROCESS

A. Arc GLOW's **Notice of Privacy Practices** contains the following information:
    1. A description of the types of uses and disclosures of protected health information that may be made for treatment, to obtain payment, or to conduct the agency's business operations;
    2. A description of what information is protected;
    3. Incidental Disclosures;
    4. Individual rights of the person; and
    5. How a person can exercise their rights.

B. At the start of services with the Arc the person supported or their personal representative will be provided a paper copy of Arc GLOW's **Notice of Privacy Practices.** The Notice of Privacy Practices is to be given to the person no later than the first service delivery date. The first department to provide service will distribute the notice. A copy of the specific **Notice of Privacy Practices** issued must be maintained in the individual's service file or a centralized location electronically.

C. The department distributing the **Notice of Privacy Practices** will make a good faith effort to obtain a signed acknowledgement form (**HIPAA Privacy Notice Acknowledgement of Receipt)** from the person. This signed acknowledgement form becomes part of the person's service file/ electronic record. Acknowledgement form should be uploaded in file attachments in the electronic health record. If the acknowledgement form is not received, the department distributing the privacy notice must document its efforts to obtain the acknowledgement and the reason why it was not obtained on the acknowledgement form.

D. Arc GLOW's current **Notice of Privacy Practices** is posted and available at Arc GLOW's Main Office located at 18 Main St., Mt Morris , at other agency service delivery locations, and on the agency website, and is available upon request.

E. If the **Notice of Privacy Practices** is revised, Arc GLOW will make the notice available upon request on or after the effective date of the revision. The Privacy Officer is responsible for any updates to the notice, communication of changes to all programs, and ensuring the updated notice is posted.

Arc GLOW

Topic: Disclosures of Protected Health Information for Treatment, Payment, and Health Care Operations	**Ref. No.** 345 – B
Department: Corporate Compliance	**Page:** 1 of 7
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/2014, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 5/2016, 10/2019, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 4/2017, 4/2018, 6/2023

PURPOSE

The purpose of this policy is to ensure awareness of HIPAA regulations and agency policy and procedures regarding protected health information (PHI, as defined below).

POLICY

Arc GLOW is committed to protecting the privacy and confidentiality of health information about the people we support. "Protected health information" (PHI, as defined below) is strictly confidential and should be used and disclosed only for those purposes authorized under the agency's policies, privacy practices, or applicable law. It is the responsibility of personnel affected by this policy to preserve the privacy and confidentiality of all protected health information and to ensure that protected health information is used and disclosed only as permitted under the agency's policies, privacy practices, and applicable law. This includes, but is not limited to, compliance with the protective procedures below. This policy applies to protected health information in any form, including spoken, written, or electronic forms.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc GLOW employees, interns, Board Members, volunteers, consultants, contractors, business associates, and subcontractors of the organization.

DEFINITIONS

Individually Identifiable Health Information

For purposes of this policy, the term “individually identifiable health information” means any health information about the people we support that was created or received by Arc GLOW and that:

1. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual **and**
2. either identifies the individual or could reasonably be used to identify the individual.

Protected Health Information

For purposes of this policy, “protected health information” is any individually identifiable health information (as defined above, whether written, oral or electronic) that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Some examples of protected health information are:

- information about the person’s health condition (such as a diagnosis the person may have);
- information about health care services the person has received or may receive in the future (such as habilitation services, Physical Therapy or Occupational Therapy);
- information about the person’s health care benefits under an insurance plan (such as whether a person receives Medicaid, or whether a prescription is covered); or
- information about whether a person is receiving health care services from Arc GLOW or any other health care provider and the type of service received;

when combined with:

- demographic information (such as the person’s name, address, date of birth, race, gender, ethnicity, or marital status);
- geographic information (such as where the person lives or works);
- unique numbers that may identify the person (such as a social security number, medical record number, telephone number, or driver’s license number); or
- other types of information that may identify who the person is.

Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C.

Health Care

For purposes of this policy, “health care” is care, services, or supplies related to the health of the individual, including, but not limited to:

- preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status of an individual, or that affects the structure or function of the body and
- dispensing of a drug, device, equipment or other item in accordance with a prescription

Use

For purposes of this policy “use” is defined as the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within Arc GLOW.

Disclosure

For purposes of this policy, “disclosure” is the release, transfer, provision of access to, or divulging in any other manner of information outside Arc GLOW.

Treatment

For purposes of this policy, the term “treatment” means providing, coordinating, or managing the person’s agency authorized health care, service provision, and any related services. Some examples of treatment activities involving the use or disclosure of protected health information are:

- using protected health information about a person’s disease or condition to diagnose or provide care to the person;
- disclosures of protected health information to other health care providers and/or covered entities who are involved in taking care of the person;
- disclosures of protected health information to another health care provider in order to obtain advice about how best to diagnose or provide care to the person; and
- disclosures of protected health information to another health care provider and/or covered entity to whom the person has been referred to ensure that this health care provider has the necessary information to diagnose or provide care to the person.

Payment

For purposes of this policy, the term “payment” generally means the activities undertaken by the agency to obtain or provide reimbursement for the provision of health care (for example, billing activities). Some examples of payment activities involving the use or disclosure of protected health information are:

- disclosing the person’s protected health information to a health insurance plan to determine whether it will provide coverage for the person’s treatment;
- disclosing the person’s protected health information to obtain pre-approval before providing a treatment or service, such as enrolling the person to the agency for a particular type of service;
- disclosing the person’s protected health information to his or her health insurance plan to obtain reimbursement after the agency has provided service to the person; and
- disclosing the person’s protected health information to review services with respect to medical necessity, appropriateness of care or justification of charges

Uses and disclosures of protected health information for the agency’s payment purposes are subject to the HIPAA Privacy Regulations’ "minimum necessary" standard. Reference HIPAA policy #345-C: Disclosures of Protected Health Information: Minimum Necessary Standard.

Health Care Operations

For purposes of this policy, the term “health care operations” generally refers to those general business and administrative functions of the agency that are required in order to operate and perform its health care functions. Some examples of uses and disclosures of protected health information for health care operations are:

- uses and disclosures of protected health information for quality assurance and utilization review purposes;
- uses and disclosures for care coordination and case management
- uses and disclosures of protected health information for education and training of personnel affected by this policy, and to review the competence and qualifications of health care professionals;
- uses and disclosures of protected health information to recommend possible treatment options or alternatives, or health-related benefits or services that may be of interest to the person;
- uses and disclosures of protected health information for legal services, business planning, and other business management and general administrative activities as defined in HIPAA regulations; and
- uses and disclosures of de-identified protected health information to raise funds for the benefit of the agency.

Uses and disclosures of protected health information for the agency’s health care operations are subject to the HIPAA Privacy Regulations’ "minimum necessary"

standard. Reference HIPAA policy #345-C: Disclosures of Protected Health Information: Minimum Necessary Standard.

Covered Entity

For purposes of this policy a "covered entity" is a health plan, a health care clearinghouse, or a health care provider that stores, processes, or transmits any health information in electronic form in connection with a transaction covered by HIPAA regulations. Arc GLOW is a health care provider considered a covered entity under HIPAA regulations.

PROCESS

A. Uses and Disclosures for Treatment, Payment, and Health Care Operations (TPO)

Protected health information may only be shared in accordance with this policy and Arc GLOW's **Notice of Privacy Practices**. Information disclosed for purposes of (i) the agency's treatment activities, payment activities, and health care operations, and (ii) certain treatment activities, payment activities, and health care operations of other health care providers and of health plans, may be shared without a person's written consent.

Disclosure to Other Covered Entity's Treatment, Payment, and Health Care Operations

Arc GLOW may disclose protected health information to others for their treatment, payment, and health care operations as follows:

- The agency may disclose protected health information to another health care provider for its treatment activities.
- The agency may disclose protected health information to a health plan or another health care provider for its payment activities.
- The agency may disclose protected health information to a health plan or another health care provider for its health care operations, but only if

  (i) both the Arc and the other party have, or had, a relationship with the person supported whose information is being disclosed;

  (ii) the protected health information being disclosed pertains to that current (or previous) relationship; and

  (iii) the disclosure is for health care operations activities, as defined above and in HIPAA regulations, including care coordination and case management; conducting quality assurance and/or quality improvement activities; education or training of students and other personnel affected by this policy; reviewing the competence, qualifications, or the performance of

health care professionals; accreditation; licensing; credentialing; and fraud and abuse detection or compliance activities.

Disclosures of protected health information for others' payment activities or health care operations are subject to the HIPAA Privacy Regulations' minimum necessary standard. Reference HIPAA policy #345-C: Disclosures of Protected Health Information: Minimum Necessary Standard.

B. De-identified Information Not Subject To Treatment, Payment, And Health Care Operations Restriction

Health information that does not identify an individual and with respect to which there is not reasonable basis to believe it can be used to identify an individual is not considered individually identifiable health information. Protected health information will be deemed de-identified when (i) a person with appropriate knowledge and experience in scientific and statistical principles for de-identifying information has determined that there is a very small risk that the information can be used to identify the person and has documented the analysis that justifies that decision, OR (ii) certain specific identifying elements regarding the person supported, his/her relatives, employers, and household members have been removed and the remaining information cannot be used to identify the person.

The elements that must be removed include the following:

- names;
- all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes;
- all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age;
- telephone numbers;
- fax numbers;
- electronic mail (e-mail) addresses;
- 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;
- World Wide Web Universal Resource Locators (URLs);
- internet protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints;
- full face photographic images and comparable images; and

- any other unique identifying number, characteristic, or code when the key is readily available.

Because de-identified information is no longer considered protected health information, such de-identified information is not subject to the treatment, payment, or health care operations restriction and generally may be used and disclosed without limitation. However, agency personnel affected by this policy must obtain approval from our agency's Privacy Officer that protected health information has been appropriately de-identified prior to treating such information as de-identified information.

C. Uses of Protected Health Information for Reasons Other Than Treatment, Payment, and Health Care Operations

Agency personnel affected by this policy are instructed to consult their supervisors if they are unsure whether a particular use or disclosure satisfies the definition of treatment, payment, or health care operations or if they believe they need to use or disclose protected health information for reasons other than treatment, payment, and health care operations and they are unsure whether an exception applies, or if the agency has obtained an authorization for that particular use or disclosure. The supervisor will use Arc GLOW's HIPAA Privacy Plan and Notice **of Privacy Practices** as a resource for providing guidance, or direct the individual to the Department Director/Vice President or Privacy Officer.

D. Unauthorized Use and Disclosure

Improper uses and disclosures of protected health information must be tracked and, in some cases, reported. Any unauthorized or improper use or disclosure of protected health information must be promptly reported to the supervisor and the Privacy Officer. The Privacy Officer is responsible for ensuring a thorough investigation and corrective actions.

Arc GLOW

Topic: Disclosures of Protected Health Information: Minimum Necessary Standard	**Ref. No.** 345 – C
Department: Corporate Compliance	**Page:** 1 of 6
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 5/2016, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

To protect the privacy of the people we support by establishing a minimum necessary standard for uses, disclosures, and requests of protected health information.

POLICY

Arc GLOW personnel affected by this policy are expected to limit their uses and disclosures of protected health information and requests for protected health information to the minimum amount of information that is reasonably necessary to perform their duties for the agency.

This expectation does not mean that agency personnel affected by this policy should restrict exchanges of information required in order to treat the people we support quickly and effectively.

Supervisors, with assistance from the Privacy Officer, are expected to help ensure that agency personnel affected by this policy make reasonable efforts to limit protected health information and requests for protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request, in relation to their duties with Arc GLOW.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc GLOW employees, interns, Board Members, volunteers, consultants, contractors, and subcontractors of our organization.

PROCESS

Routine Activities

Personnel of the organization affected by this policy routinely use protected health information about the people we support to carry out their duties. They may also need to disclose protected health information about the people we support to persons outside the organization, or to request protected health information from these persons. Arc GLOW believes that the personnel affected by this policy should have the minimum amount of information necessary for them to carry out their daily duties, in accordance with this Privacy Plan and our **Notice of Privacy Practices**. At any time in which information about a person supported by Arc GLOW must be shared with others, they must be able to demonstrate the need to know. The need to know can be determined by evaluating whether the safety and quality of service they are providing to a person would suffer greatly without having the information. All are expected to follow this standard at all times. These practices have been carefully developed and are not intended to limit any communications required for Arc GLOW personnel affected by this policy to provide quick, effective, and high-quality services.

Questions about how the minimum necessary standard should be applied in a particular situation should be directed to Supervisors, Directors/Vice Presidents, or the Privacy Officer.

Non-Routine Situations

There may be situations that arise that do not qualify as routine situations, such as situations which involve personal health information about people we support that do not clearly fall within the daily duties of Arc GLOW personnel affected by this policy. If the general practices do not address a particular situation or do not permit use, disclosure, or the request of protected health information in a way that is necessary to carry out duties, the Department Director /Vice President should be notified. The Director /Vice President will be responsible for providing guidance or, if necessary, consulting with the Privacy Officer to determine how much information may be used, disclosed, or requested. Individual Arc GLOW personnel affected by this policy should not make decisions on their own if the situation is not covered in policy or procedure.

In addition, Directors/Vice Presidents/Designees are expected to follow the minimum necessary standard when consulted by personnel affected by this policy who believe that protected health information must be used, disclosed, or requested in a way that is not covered by policy or procedure.

A. Uses of Protected Health Information

Arc GLOW personnel affected by this policy are instructed to notify their Department Director/Vice President/Designee if they believe they need to *use* protected health information in a way that is not addressed by the agency's

policies or procedures. The Director/Vice President/Designee will be responsible for providing guidance or, if necessary, directing the person seeking clarification to, or consulting with Arc GLOW's Privacy Officer to determine how much information may be accessed and used to appropriately address the situation and by whom. The Privacy Officer and Director/Vice President/Designee should follow the minimum necessary standard when making this decision. If there is insufficient time to consult with the Privacy Officer without jeopardizing care to the people we support, the Director/Vice President/Designee may make this determination on his/her own and notify the Privacy Officer as soon as possible afterwards.

B. Disclosures of and Requests for Protected Health Information

Arc GLOW personnel affected by this policy are instructed to contact their Department Director/Vice President/Designee if they believe they need to *disclose* or *request* protected health information in a way that is not addressed by the agency's policies or procedures. The Director/Vice President/Designee will be responsible for providing guidance or, if necessary, directing the person seeking clarification to or consulting with Arc GLOW's Privacy Officer. The Privacy Officer should then determine what information might be disclosed or requested according to the below procedures. If there is insufficient time to consult with the Privacy Officer without jeopardizing care to the people we support, the Director/Vice President/Designee may make this determination on his/her own and notify the Privacy Officer as soon as possible afterwards.

Many disclosures to persons outside the agency, or requests for information from persons outside the agency will require a written authorization from the person we support whose protected health information is involved. This policy discusses only how much information may be disclosed or requested, and does not discuss when such authorizations are required. Refer to Policy # 345- K- Individual Authorizations for Release of PHI and Arc GLOW's **Notice of Privacy Practices** for more information on required authorizations.

1. Disclosures in Response to Requests from Selected Persons

When the following persons or organizations are making a request, the Supervisor/Director or Privacy Officer may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose.

- Professionals within the organization who also provide services to the person and have represented that the information requested is the minimum necessary for the stated purpose.
- Business Associates of Arc GLOW who have represented that the information requested is the minimum necessary for the stated purpose and who have agreed in writing (via a **Business Associate Agreement**) to appropriately safeguard the information.

- A health care provider that is required to comply with federal privacy regulations.
- A health plan that provides or pays the cost of medical care and is required to comply with federal privacy regulations.
- A health care clearinghouse that converts health information to and from standard and non-standard formats and is required to comply with federal privacy regulations.
- A researcher with appropriate documentation from an Institutional Review Board (IRB), or Privacy Board, that meets the requirements of the agency's policy regarding uses and disclosures of protected health information for research purposes.
- A public official or agency requesting protected health information for a public policy purpose if the public official represents that the information requested is the minimum necessary for the stated purpose.

If the Supervisor or Privacy Officer strongly believes that a request by one of the foregoing persons or organizations seeks more than the minimum information necessary, he/she should attempt to reach a compromise that meets the concerns and needs of both Arc GLOW and the person or organization making the request.

2. Disclosures in Response to All Other Requests

If the authorized request is made from any other person or organization, the Supervisor or Privacy Officer should decide how much information to disclose, using the following criteria:

- What is the *purpose* of the disclosure?
- What *type* of information does the recipient need to accomplish the purpose of the disclosure?
- Where is this information *located*? For example, is it in a medical record? Is it on an electronic database?
- Is other information *attached* to this information? If so, is the attached information also needed to accomplish the purpose of the disclosure? *If the attached information is not needed, a copy of the record should be made, and the extraneous information should be redacted.*

3. Requesting Protected Health Information from Others

When deciding what information may be requested from another person or organization outside the agency, the Supervisor or Privacy Officer should consider the following criteria:

- What is the purpose of the request?
- What type of information does the agency need to accomplish this purpose? This may require consultation with the department director.

- What other information is likely to be attached to the information the agency is requesting? *If that information is not needed, the Privacy Officer should specify in the request that this information need not be disclosed.*
- Can the request be phrased more *narrowly* to target only the information needed by the agency to accomplish this purpose?

C. Limitations on Using, Disclosing, or Requesting the Entire Medical Record

Arc GLOW personnel affected by this policy may not use, disclose, or 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 use, disclosure, or request. Personnel affected by this policy are instructed to contact their Department Director/Vice President/Designee if they believe that the entire medical record should be used, disclosed, or requested. The Director/Vice President/Designee will be responsible for consulting with the agency's Privacy Officer to determine whether there is a specific justification for using, disclosing, or requesting the entire record. If there is insufficient time to consult with the Privacy Officer without jeopardizing care to the person we support, the Director/Vice President/Designee may make this determination on his/her own and notify the Privacy Officer as soon as possible afterwards. The specific justification for using, disclosing, or requesting the entire record should always be documented in the person's record.

D. Special Requirements for Using, Disclosing, or Requesting Certain Types of Information

Arc GLOW personnel affected by this policy are advised that special concerns are raised when using, disclosing, or requesting certain types of information, particularly alcohol and substance abuse information, psychotherapy information, and HIV-related information. Specific processes addressing these types of information should be consulted when these types of information are involved.

E. Exceptions

The following uses, disclosures, and requests are not limited by the minimum necessary standard explained in this policy. The Supervisor or Privacy Officer nevertheless should do his/her best to limit the amount of information used, disclosed, or requested in these situations to what is appropriate under current medical and ethical guidelines.

- *Requesting* information from or *disclosing* information to, another health care provider for treatment purposes regarding the people we support.
- *Disclosing* information to the person we support or to a personal representative who is authorized to make health care decisions for that person.
- *Using* or *disclosing* information about a person we support pursuant to an authorization requested by that person.

- *Disclosing* protected health information as required by U.S. Department of Health and Human Services in connection with its investigation or determination of the agency's compliance with the HIPAA Privacy Regulations.
- *Using* or *disclosing* protected health information as required by law (not just using or disclosing in a manner that is permitted by law).

Arc GLOW

Topic: Confidentiality Standards for Protected Health Information	**Ref. No.** 345 – D
Department: Corporate Compliance	**Page:** 1of 3
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 5/2016, 4/2018, 1/2022, 6/2023
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 4/2017, 10/2019

PURPOSE

The purpose of this policy is to ensure all personnel are aware of their responsibility to protect the privacy and preserve the confidentiality of all protected health information (PHI), as defined in Policy # 345-B – Disclosures of Protected Health Information for Treatment, Payment and Health Care Operations. This includes, but is not limited to, compliance with the policy and protective procedures below.

POLICY

Arc GLOW is committed to protecting the privacy and confidentiality of health information about the people we support. Protected health information is strictly confidential and should never be given nor confirmed to anyone who is not authorized under the minimum necessary standard, in accordance with Policy # 345-C, other HIPAA policies, or the law to receive this information. Confirmed in this context means verifying that an individual receives services from the Arc, that an individual has a particular diagnosis, or that an individual lives or works in a specific location. Personnel affected by this policy are granted access to protected health information based on their assigned functions, and access privileges should not exceed those necessary to accomplish the assigned functions. This policy applies to protected health information in any form, including spoken, written, or electronic.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc GLOW employees, interns, Board Members, volunteers, consultants, contractors, and subcontractors of the organization.

PROCESS

A. Public Viewing/Hearing

Arc GLOW personnel affected by this policy are expected to keep protected health information out of public viewing and hearing. For example, protected health information should not be left in conference rooms, out on desks, on copiers or printers, or on counters or other areas where the information may be accessible to the public or to other individuals who do not have a need to know the protected health information. Arc GLOW personnel affected by this policy should also refrain from discussing protected health information in public areas, such as hallways and reception areas; unless doing so is necessary to provide emergency treatment to one of the people we support. Arc GLOW personnel affected by this policy should also take care in sharing protected health information with families and friends of the people we support. Such information may generally only be shared with a person's "personal representative" or to a person's family member, relative, or close personal friend who is involved in their care. Even in the latter circumstance, information cannot be disclosed unless the person has had a chance to agree or object to the disclosure, and personnel may only disclose information that is relevant to the involvement of that family member, relative, or close personal friend in the person's care or payment for the person's care, as the case may be.

B. Databases and Workstations

Arc GLOW personnel affected by this policy are expected to ensure that they exit any confidential database and email accounts upon leaving their workstations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. Personnel affected by this policy are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including but not limited to, any password, personal identification number, token or access card, or electronic signature. All Arc GLOW personnel affected by this policy will be liable for all activity occurring under his or her account, password, and/or electronic signature. These activities may be monitored and will be checked if necessary to determine whether or not a breach occurred.

C. Downloading, Copying, or Removing Records

Arc GLOW personnel affected by this policy should not download, copy, or remove from the agency any protected health information, except as necessary to perform their duties at Arc GLOW. Removal of records requires the prior approval of the supervisor with authority over the records. Personnel affected by

this policy are responsible for the safeguarding of any agency records in their possession. No records may be left unattended or unsecured in a manner that will allow access by unauthorized parties. Personnel affected by this policy must report the loss or destruction of any records immediately to the supervisor with authority over the records. Upon termination of employment or contract with the organization or upon termination of authorization to access protected health information, personnel affected by this policy must return to the agency any and all copies of protected health information in their possession or under their control.

D. Record Storage

Arc GLOW personnel affected by this policy must maintain and store all records containing PHI or pertaining to persons supported in a secure area, accessible only by those with authorized access to the records. Records stored in general areas must be locked at all times when no authorized personnel are present. No PHI may be left unattended or shared with other authorized personnel in a manner that would be visible to unauthorized personnel. Confidential information needed for meetings should be viewed at the meeting and retrieved at the end for appropriate safeguarding and storage. Committee members who maintain records of meetings must ensure their safeguarding at all times, and must return any records to the agency for destruction upon separation from the committee.

E. Emailing and Faxing Information

Arc GLOW personnel affected by this policy should not transmit protected health information over the Internet (including email) and other unsecured networks unless using a secure encryption procedure or unless requested to do so in writing by a person authorized to provide consent who has been informed of the risks involved with and agreed in writing to such transmission. Personnel affected by this policy may transmit protected health information over the agency's Intranet (email addresses ending in "ArcGLOW.org") securely within the agency's network.

Transmission of protected health information is permitted by fax only if Arc GLOW personnel affected by this policy sending the information ensure that the intended recipient is available to receive the fax as it arrives, or confirms that there is a dedicated fax machine that is monitored for transmission of sensitive information. Arc GLOW personnel affected by this policy should use fax cover sheets that include standard confidentiality notices and should request that the recipient call the sender of the fax to confirm receipt. If personnel are expecting a confidential fax, they should be available to retrieve it promptly from any public area.

F. Mailed Information

Arc GLOW personnel designated to distribute mail within the agency must take care to ensure that mail is delivered to the correct recipient. All personnel should clearly mark the name and department of the person a mail item is intended for on agency interoffice envelopes, ensuring that all other names are crossed off. If personnel affected by this policy inadvertently receive mail that is not intended for them, it is their responsibility to immediately notify the person for whom the mail was intended, and discuss delivery of the item. Personnel are expected to remove mail from mailboxes on a regular basis and designate someone to retrieve their mail during extended absences. No one should open the mail of others unless authorized to do so by the appropriate administrator.

G. OPWDD Auditor/Surveyor Access to Records

Auditors/Surveyors have the right to request and access records for those we support, as our oversight entity. When providing auditors/surveyors access to electronic records, Arc GLOW has key staff to ensure access is limited to only those records and information that are included in the scope of the audit. These key staff include members of the Information Technology (IT) team, members of the Quality and Compliance team, and the QA Technician. If auditors/surveyors are granted wide access to the electronic records, their access will be monitored by designated program supervisory staff.

Arc GLOW

Topic: Privacy of Psychotherapy Notes	**Ref. No.** 345 – E
Department: Corporate Compliance	**Page:** 1 of 4
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (As Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 5/2016, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

The purpose of this policy is to protect the privacy of psychotherapy notes about the people supported by Arc GLOW.

POLICY

It is Arc GLOW's policy that all employees become familiar with the HIPAA requirement that psychotherapy notes should be given heightened privacy protection because of the sensitivity of their contents and the atmosphere of trust between a therapist and person supported that is required for effective psychotherapy. This policy lists the situations in which psychotherapy notes may be used or disclosed without authorization from the person supported. ***Except in the specific situations listed below, authorization by the person supported is required before using or disclosing these notes.*** In addition, the person supported is not permitted to access or amend psychotherapy notes. Arc GLOW employees providing mental health services are expected to comply with this policy.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc GLOW employees, interns, Board Members, volunteers, consultants, contractors, business associates, and subcontractors of the organization, but primarily affects those who provide clinical psychotherapy or counseling services.

PROCESS

A. Records That Qualify as Psychotherapy Notes

Psychotherapy notes are notes recorded by a health care provider who is a mental health professional that document or analyze the contents of a

conversation during a private counseling session or during a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. These notes have sometimes been referred to as "process notes" (not to be confused with "progress notes"). The notes capture the mental health professional's impressions about the person supported and contain details of the psychotherapy conversation considered to be inappropriate for inclusion in the medical/clinical record. Such notes are intended to be used by the mental health professional to help him or her recall the therapy discussion and are of little or no use to others not involved in the therapy. With very limited exceptions, information in these notes is not intended to be communicated to, or even be seen by, persons other than the mental health professional who created them. These notes are therefore kept separate from the rest of the medical/clinical record.

If mental health professionals keep psychotherapy records, those professionals are expected to maintain any and all psychotherapy notes separate from the person's medical/clinical record. Only such notes are entitled to the special protections set forth in this policy. If for any reason psychotherapy notes are inadvertently included in the medical/clinical record, they will no longer be subject to the protections of this policy. Arc GLOW personnel affected by this policy should therefore make all reasonable efforts to ensure that these notes are not mistakenly included in the person's medical/clinical record.

B. Records That Do Not Qualify as Psychotherapy Notes

Certain types of mental health records *do not* qualify for the protection given to psychotherapy notes. These are:

- Medication prescription and monitoring;
- Counseling session start and stop times;
- Modalities and frequencies of treatment furnished;
- Results of clinical tests;
- Any summaries of the person's diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date; and
- Any information typically needed for treatment, payment, or health care operations.

These records are usually included in the person's medical/clinical record. These are not given the same heightened privacy protection available for psychotherapy notes for two reasons. First, it is important that the originator of these records be permitted to disclose these records when necessary for proper treatment of the person, for payment, and for health care operations of the agency. Second, people supported have heightened interest in access to these records, which are used to make treatment decisions about them. These records are therefore subject to ordinary privacy protections which generally (1) permit use and disclosure in accordance with Arc GLOW's HIPAA Privacy Plan and

Notice of Privacy Practices and (2) permit access unless denied on other grounds under the agency's policies. Arc GLOW personnel providing mental health services should use and disclose these records in accordance with the agency's policies concerning the privacy of all other types of protected health information about the people we support.

C. Use and Disclosure of Psychotherapy Notes

Psychotherapy notes may only be used and disclosed as described below. To the extent that any provision of any other Arc GLOW policy conflicts with the provisions in this policy, this policy governs.

1. Authorization of the Person Supported Not Required

Creator of Notes: Psychotherapy notes may be used by the mental health professional that created them in order to treat a person who is the subject of the notes.

- A mental health professional is *not permitted*, however, to use *another* mental health professional's psychotherapy notes in order to provide treatment to a person, even if the other mental health professional is a member of the organization's workforce.
- The creator of the psychotherapy notes is also *not permitted* to use them for payment or health care operations (except for training discussed below). The person's specific authorization for such uses and disclosures is required.

Students and Trainees: Psychotherapy notes may be used by or disclosed to students, trainees, or practitioners in mental health who are learning under supervision to practice or improve their skills in group, joint, family, or individual counseling.

- A mental health professional, however, is *not permitted* to share his/her psychotherapy notes with medical students or trainees who are *not* in training to provide mental health services.

Threat to Health or Safety: Psychotherapy notes may be used or disclosed when a mental health professional who created the notes determines that such 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, so long as any disclosure is made to a person who is reasonably able to prevent or lessen the threat.

Legal Action: Psychotherapy notes may be used or disclosed to defend a legal action or other proceeding brought by the person against the creator of the notes, Arc GLOW, or its personnel affected by this

policy. This includes disclosures to outside legal counsel.

- This exception *does not permit* the use or disclosure of psychotherapy notes in a legal action brought by the person against another health care provider outside the organization.
- This exception also *does not permit* the use or disclosure of psychotherapy notes to defend the creator of the notes, Arc GLOW, or its personnel affected by this policy in a legal action brought by someone other than the person who is the subject of the psychotherapy notes.

Required by Law: Psychotherapy notes may be used or disclosed without authorization of the person when Arc GLOW's Privacy Officer determines that such use or disclosure is required by law, and the use or disclosure complies with and is limited to the relevant requirements of such law.

Health Oversight Agencies: Psychotherapy notes maintained by Arc GLOW may be used or disclosed without authorization of the person when the agency's Privacy Officer determines that such use or disclosure is required to provide information requested by the United States Department of Health and Human Services in order to investigate whether Arc GLOW or the mental health professional who created the notes has complied with the HIPAA Privacy Regulations.

Medical Examiners and Coroners: Psychotherapy notes may be used or disclosed when the Privacy Officer determines that such use or disclosure is necessary to provide information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law.

2. Authorization of the Person Supported Is Required

In all other cases, the person's authorization is required before using or disclosing psychotherapy notes.

Agency personnel affected by this policy may *not* combine a person's specific authorization to use or disclose psychotherapy notes with any other document except for another authorization to use and disclose psychotherapy notes. For example, a written authorization to use and disclose the information contained in psychotherapy notes may not be made a part of, or even paper-clipped or stapled together with, a general written consent or written authorization permitting the use or disclosure of other types of individual information or any informed consent document. These documents must be presented to the individual and signed by the individual one at a time.

D. Individual Access to and Amendment of Psychotherapy Notes

It is the policy of Arc GLOW that the people we support shall not be granted access to psychotherapy notes. A person's request for amendment of psychotherapy notes should be denied as well. Arc GLOW employees who provide mental health services should
refer all requests to access or amend psychotherapy notes to the Privacy Officer for processing in accordance with HIPAA policies #345-H (Individual Access to Protected Health Information) and #345-J (Individual Requests to Amend Protected Health Information). These policies provide specific time lines and documentation requirements for denying these requests made by people we support.

Arc GLOW

Topic: Privacy of Human Immunodeficiency Virus (HIV)-Related Information	**Ref. No.** 345 – F
Department: Corporate Compliance	**Page:** 1 of 5
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 4/2015, 4/2018, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 5/2016, 4/2017, 10/2019, 6/2023

PURPOSE

The purpose of this policy is to ensure the protection of individuals we support in relation to the confidentiality of HIV-related information.

POLICY

Arc GLOW is committed to protecting the privacy and confidentiality of health information of the people we support. Use and /or disclosure of confidential HIV-related information will be consistent within these HIPAA policies with the use and/or disclosure of any protected health information, and in accordance with New York State Public Health Law Article 21, Title 3 and Article 27-F.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc GLOW employees, interns, Board Members, volunteers, consultants, contractors, business associates and subcontractors of our organization who need to disclose or receive confidential HIV-related information.

DEFINITIONS

N.Y. Public Health Law defines four relevant categories of disease, illness, or procedure relevant to HIV and AIDS: (I) AIDS is defined to mean “acquired immune deficiency syndrome, as may be defined from time to time by the Centers for Disease Control and Prevention of the United States Public Health Service.” (ii) “HIV infection” is defined to mean “infection with the human immunodeficiency viruses that are the cause of AIDS or as the term may be defined from time to time by the Centers for Disease Control and Prevention of the United States Public Health Service.” (iii) “HIV-related illness” is defined to mean “any clinical illness that may result from or be associated with HIV infection”; and (iv) “HIV-related test” is defined to mean “any laboratory test or

series of tests for any virus, antibody, antigen, or etiologic agent whatsoever thought to cause or to indicate the presence of HIV infection, HIV-related illness or AIDS".

'Confidential HIV-related information" is defined to mean "any information, in the possession of a person who provides one or more health or social services or who obtains the information pursuant to a release of confidential HIV related 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".

PROCESS

A. Disclosures of Confidential HIV-Related Information

Release/disclosure of HIV-related information is only allowed pursuant to written authorization by the person that is supported by Arc GLOW, or when the person lacks capacity to consent, a person authorized pursuant to law to consent to health care of the individual. No person who obtains confidential HIV-related information in the course of providing any health or social service or pursuant to an authorized release of confidential HIV-related information may disclose or be compelled to disclose such information, except to the following:

1. The protected individual or, when the person lacks capacity to consent, a person authorized pursuant to law to consent to health care for the individual.
2. Any person to whom disclosure is authorized pursuant to a specific, written release of confidential HIV-related information which includes a statement prohibiting re-disclosure.
3. An agent or employee of Arc GLOW or other health facility if they are authorized to access medical records, if the agency is authorized to obtain HIV-related information, and if personnel affected by this policy provide health care to the protected individual, or maintain or process medical records for billing or reimbursement.
4. Arc GLOW personnel affected by this policy who need the information in order to provide care to the people supported by our agency.
5. Accreditation or oversight review organizations authorized to access medical records, if they only disclose the information back to Arc GLOW to carry out the monitoring, evaluation, or service review for which it was obtained or to a federal, state or local government agency for the purposes of and pursuant to their regulations. Private organizations performing accreditation services for Arc GLOW should have a Business Associate Agreement.
6. A federal, state, county or local health officer when such disclosure is mandated by federal or state law.

7. Adoption and Foster Care Agencies or other corporations authorized by Social Services Law, Section 371, to receive children for adoption or foster care, in connection with foster care or adoption of a child. Authorization from the person's appropriate legal representative of a child should be obtained before disclosing the confidential HIV-related information to an adoption or foster care agency that does not have the authority under applicable law to make health care decisions on behalf of the child. If the agency is disclosing confidential HIV-related information about the child's parent to the adoption or foster care agency in connection with the adoption or foster care placement, an **Individual Authorization to Release PHI** (with HIV-Related Information clearly selected) should be obtained from the child's parent before making the disclosure unless the disclosure is otherwise required by law.

8. A Law Guardian appointed to represent a minor pursuant to the social services law or the family court act, for the purpose of representing the minor. If the minor has the capacity to consent, the law guardian may not re-disclose confidential HIV related information without the minor's permission. If the minor lacks capacity to consent, the law guardian may re-disclose confidential HIV related information for the purpose of representing the minor. If a law guardian does not have the authority under applicable law to make health care decisions on behalf of the minor and if the disclosure is not required by the legal appointment of the law guardian, an **Individual Authorization to Release PHI** (with HIV-Related Information clearly selected) must be obtained.

9. Insurance Institutions for Non-Payment Purposes: An **Individual Authorization to Release PHI** (with HIV-Related Information clearly selected) must be obtained before disclosing confidential HIV-related information to insurance institutions for non-payment purposes.

10. Division of Parole, Division of Probation and Correctional Alternatives, or Commission of Corrections, in order to carry out functions, powers and duties with respect to the protected person and in accordance with Public Health Law Article 27-F.

11. The Medical Director of a local Correctional Facility in accordance with Public Health Law Article 27-F, to the extent the medical director is authorized to access records to carry out his / her functions relating to the protected individual. Re-disclosure by the medical director is prohibited except as permitted under Public Health Law Article 27-F, Article 21, Title III and implementing regulations.

12. A health facility or health care provider, in relation to the procurement, processing, distributing or use of a human body or a human body part, including organs, tissues, blood, semen, or other body fluids, for use in medical education, research, therapy, or for transplantation to individuals.

13. Third party reimbursers or their agents to the extent necessary to reimburse health care providers, including health facilities, for health services, provided that an otherwise appropriate authorization for such disclosure has been secured.

14. To a funeral director upon taking charge of the remains of a deceased person when such funeral director has access in the ordinary course of business to HIV-related information on the death certificate of the deceased individual, as authorized by Public Health Law Section 4142.
15. Any person to whom disclosure is ordered by a court of competent jurisdiction pursuant to Public Health Law Section 2785.
16. An employee or agent of the New York City Board of Corrections so that the board may continue to access records of inmates who die while in the custody of the New York City Department of Corrections when necessary for the board to carry out its duties, functions, and powers with respect to the protected individual, pursuant to the New York City charter.
17. An executor or administrator of an estate of a deceased person as needed to fulfill his or her responsibilities/duties as an executor or administrator.
18. Child Protective and Adult Protective Services**:** Disclosure of confidential HIV-related information can be done where necessary to comply with reporting requirements to child protective services that are authorized or required by law or to comply with reporting requirements to adult protective services that are required by law. When a disclosure to adult protective services is not mandatory under New York law, the program should obtain the person's **Individual Authorization to Release PHI** (with HIV-Related Information clearly selected).

B. Required Documentation of HIV-Related Disclosures

1. Confidential HIV-related information shall be recorded in the medical record such that it is readily accessible to provide proper care and treatment.
2. All disclosures of confidential HIV-related information must be noted in the record. However, only initial disclosures to insurance institutions must be noted. Notation is not required for disclosure to agents or employees of health facilities or health care providers as outlined in A. 3 of this policy. Notation is not required for persons engaged in quality assurance, program monitoring or evaluation, or for governmental payment agents acting pursuant to contract or law.
3. Confidential HIV-related information shall be noted, as appropriate, in a certificate of death, autopsy report or related documents prepared pursuant to Public Health Law, Article 41 or other laws relating to documentation of cause of death.
4. The protected person shall be informed of disclosures of HIV information upon request of the protected person.
5. Confidential HIV-related information shall not be disclosable pursuant to Public Officers Law, Article 6 (the Freedom of Information Law).

Arc GLOW

Topic: Designated Record Set	**Ref. No.** 345 – G
Department: Corporate Compliance	**Page:** 1of 2
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as (Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 5/2016, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

The purpose of this policy is to document the general categories and types of records that will be considered part of a person's designated record set.

POLICY

Arc GLOW personnel affected by this policy are responsible for preparing and maintaining a designated record set for each individual that receives our services, in accordance with regulations and accepted practices.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc GLOW employees, interns, Board Members, volunteers, consultants, contractors, business associates, and subcontractors of the organization, who create and/ or maintain health care records of individuals receiving services.

PROCESS

A designated record set is a group of records maintained by Arc GLOW or for Arc GLOW by a Business Associate that contains protected health information and may be used to make decisions about people we support and their treatment. For purposes of this policy, "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for Arc GLOW.

Some records that are part of the designated record set are:

- medical and treatment records maintained by the Arc or a business associate

- billing records maintained by the Arc, such as individualized plans or billing case notes
- health plan information,
- all other documents that may be used, in whole or in part, to make decisions about individuals.

Systemic information, such as quality assurance reports and program responses, and compliance related investigations are not considered part of the designated record set because they are only used for systemic or process changes. They are not typically used to make decisions or changes to the care or treatment of individuals.

Psychotherapy notes and information compiled for legal proceedings as defined by HIPAA regulations are also not considered part of the designated record set.

The designated record set will be maintained three different ways:

1. Department Active - These are the current records of a person and are kept at the site where they receive their service. These files are up to two years old.
2. Agency Active - These are the records of a person that we continue to support at Arc GLOW that are older than two years.
3. Inactive Files - These are files of a person that is no longer supported by Arc GLOW but are required to be kept in accordance with record retention requirements

The person's Individualized Service Plan/ Life Plan, and the person can assist in providing the information regarding which departments have personal health information records which pertain to that person.

Accessing the Designated Record Set

Refer to policy on Individual Access to Protected Health Information (#345-H) for information on how to access a person's designated record set.

Arc GLOW

Topic: Individual Access to Protected Health Information	**Ref. No.** 345 – H
Department: Corporate Compliance	**Page:** 1of 12
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 4/2015, 5/2016, 4/2018, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2017, 10/2019, 6/2023

PURPOSE

Individuals generally have a right of access to inspect and obtain a copy of their own protected health information (PHI) contained in a designated record set that may be used to make decisions about them. They also have the right to request that the information be transmitted directly to another person, as long as the request is in writing, signed by the individual and clearly identifies the designated person and where to send the copy of protected health information. The purpose of this policy is to ensure this right is exercised in accordance with HIPAA regulations.

POLICY

It is the agency's policy to treat all individual requests to access information in a respectful manner. Information that has already been distributed to the people we support such as service/support plans can be reviewed with the person at his/her request. If a person we support wants to view documentation about them, staff should feel comfortable in doing so with the expectation that they assist the person in understanding what the documentation means.

If a person we support and/or their legal representative wants copies of documentation about the person or wishes to review more than just what is reasonably available, staff should contact their supervisor, as a more formal request may be required.

Arc GLOW has strict policies and procedures mandated by state and federal law about how and when individuals may access agency records. Therefore, all individual requests for access to medical records, billing records, or any other records (whether or not they contain individual health information) should be forwarded to the agency's Privacy Officer or Designee within 1 business day.

Personnel affected by this policy are expected to respond to such individual requests in a timely and respectful manner in accordance with the process below, informing the individual that the request will be forwarded to the agency's Privacy Officer.

Personnel responsible for complying with this policy should be aware that special privacy protections apply to HIV-related information, alcohol and substance abuse information, and some mental health information. Some steps which are permitted or required under this policy may not be permitted when using or disclosing these types of information. Personnel affected by this policy must comply with HIPAA Policy #345-F: Privacy of HIV-Related Information and #3435-E: Privacy of Psychotherapy Notes when processing requests involving these sensitive types of information. Personnel affected by this policy are expected to be aware of the requirements under those policies. When requests are made for access to designated record sets that contain these types of information, the Privacy Officer must consult the other policies as well.

POSITIONS PRIMARILY AFFECTED

This policy applies to the entire agency workforce, including all employees, interns, Board Members, volunteers, consultants, business associates, contractors, and subcontractors at the agency**.** All must be aware of the requirements of this policy to ensure that the right to access PHI is protected and enforced.

General knowledge of this policy is needed by all personnel affected by this policy; however, the focus should primarily be for those responsible for individual records, including, but not limited to, the person's Case Manager, Clinicians, agency Supervisors or Directors, and the Privacy Officer.

PROCESS

A. Right to Access Records

What Information: People supported have the right to inspect and obtain a copy of the protected health information that Arc GLOW, or one of its business associates, maintains in a "designated record set". A "designated record set" is a group of records maintained by or for Arc GLOW that may be used to make decisions about a person or the treatment or services he/she receives. The designated record set for each individual generally includes the individual's medical records and billing records. The specific records included in a designated record set are discussed in HIPAA Policy #345-G: Designated Record Set.

For How Long: People have the right to access their protected health information for as long as the information is contained in their designated record set.

Exceptions: In some circumstances, we may/must deny a person the right to access protected health information in his/her designated record sets. These

circumstances are discussed below in reasons for denial.
Requests by Committees or Guardians: If the request for access to records was made by a surrogate decision making committee or a legal guardian of a developmentally disabled person, and the committee or legal guardian has authority to make health care decisions for the person, and the person is 18 years of age or older, we will notify the person that the request has been made.
In Writing: All requests for access must be made in writing. Personnel affected by this policy should encourage the person or the person's personal representative to complete Arc GLOW's **HIPAA Privacy Rights Request** form or to write a letter that covers the same information requested on that form.
Follow Up Questions: Although a person's request should be made in writing, personnel responsible for the individual records are encouraged to follow up on a person's request in person or by phone if necessary to clarify what information the person is seeking to access. Personnel responsible for the individual records should record on the person's request form the results of that discussion and sign his/her notes before forwarding the request to the Privacy Officer.

B. Response Time

Arc GLOW personnel affected by this policy are expected to respond to a person's requests for access to their protected health information by immediately informing them that their request must be in writing and assisting them with accessing or completing the **HIPAA Privacy Rights Request** form or a letter containing all the elements on the form. If the person's written request is made on a letter or other document instead of the form provided, the person receiving the request should write in the equivalent information on the letter or other document, and initial and date the change.

The above form / letter should be forwarded to the Privacy Officer / Designee within 1 business day after the request is received. The Privacy Officer / Designee will review the request within 5 business days, and grant or deny access within 30 days from the date of receipt, in accordance with HIPAA regulations. The Privacy Officer will inform the requester of the decision and any associated fees if access is granted. If the agency is unable to take action within 30 days, due to extenuating circumstances, the time may be extended for no longer than another 30 days. To ensure that these deadlines are met, personnel responsible for individual records and the Privacy Officer should complete the information sections "for Arc GLOW use only" on the **HIPAA Privacy Rights Request** form.

Inspection of Records: If the person is seeking to inspect his/her information, and this has been approved by the Privacy Officer, the person responsible for the records is expected to arrange for this opportunity with the requester within 10 days from the date the request was received by the organization, in accordance with NYS Public Health Law 18.

Copies of Records: If a person is seeking a copy of his/her information and this has been approved by the Privacy Officer, the person responsible for the records will be notified and is expected to make every reasonable effort to make copies within 30 days in the form and format requested by the individual, if it is readily producible. If it is not readily producible, it must be provided in a readable hard copy or electronic format as agreed upon by the individual. The person responsible for individual records may have a one-time extension of 30 days to copy records if the department is experiencing unusual difficulty responding within the time frames above.

If a 30-day extension is needed, the person responsible for individual records must notify the Privacy Officer, who will notify the individual in writing to explain the reason for the delay and the date the agency expects to answer the person's request.

These deadlines set outside limits. The Privacy Officer and person responsible for individual records are strongly encouraged to respond to requests as soon as possible to ensure individual satisfaction with our services.

C. Process for Granting Individual Requests for Access

A person's request for access to his/her protected health information may only be granted according to the following process.

Response times in Section B of this policy must be followed, unless the person chooses to delay access until a later time for his/her own convenience. The person responsible for the records and/ or receiving the request should work closely with the Privacy Officer to ensure that people may exercise their rights in a respectful and timely manner.

1. Notify The Person: The Privacy Officer will notify the person that his/her request for access is being granted. The person may be notified in person, by phone, or in writing. If the person requested a copy of the records, the person responsible for the records should work with the Privacy Officer to make an effort to provide a copy to the individual when providing the notice informing the person that the request has been granted, or promptly thereafter. If the person requested an opportunity to inspect his/her records, the Privacy Officer must explain how the person may arrange an appointment to visit the agency and review the information.

2. Arrange for and Grant Approved Access

Requests for Inspection of Records: If the agency is granting a person's request to inspect his/her protected health information, the person responsible for the records must arrange an appointment with the individual to review his/her records and is expected to be present during inspection to ensure the safeguarding of the information. Copies cannot be provided in lieu of

inspection unless (1) the person agrees, or (2) grounds for denial in Section D of this policy justify providing copies instead of inspection.

- **Proper Identification:** The person must present proper identification before being permitted to inspect his/her information. If the person requesting to inspect the information claims to be a personal representative of the person supported, proof of the person's relationship to the person supported and authority to access records as a personal representative must be presented. The person responsible for a person's records should review and be familiar with who may support as a personal representative for the person supported.
- **Assisting with Review:** The person responsible for a person's records may ask the individual whether an appropriate clinician or other personnel affected by this policy involved in the provision of treatment or services may assist the person in reviewing the information requested. The person is free to refuse and cannot be penalized or denied access for doing so.
- **Supervising a Person's Independent Review:** If the person is not reviewing his/her information jointly with a clinician or other personnel involved in the provision of treatment or services, the person responsible for the person's record should be present in the room at all times to ensure that the integrity of the records is maintained. The person responsible for the person's record should remain in view of the person to prevent inappropriate tampering, but far enough so that the person is afforded appropriate privacy when reviewing the content of his/her records. The person responsible for the person's record should not answer any questions regarding the content of the medical record. **If the person wishes to be completely alone, he/she must request copies of the records.**
- **Fees:** The Arc may not charge the person a fee in connection with inspection of his/her records in our designated record set.
- **Other Issues:** A person's review of his/her information should take place only where the person will not be able to view information or records concerning other persons supported by Arc GLOW. A person may be accompanied by a family member or other individual and may view his/her records with that companion.

Requests for Copies: Whenever possible, copies of records should be provided in the form or format requested by the person. For example, if the person requests that the information be sent by electronic mail, the person responsible for the records should provide the information by secure electronic mail if possible.

- If the information cannot be easily produced in the format requested by the person, the person responsible for the records may either provide the person with a readable hard copy or electronic form that is acceptable to the person.
- Copies should be delivered to the person in the method specified on the person's request form or letter. The person may visit the agency to pick up

the copies or request that the copies be delivered by mail or by secure electronic mail to an address provided on the form or letter. If delivered by mail, ensure return receipt option is used.

Providing Summaries or Explanations: If the person's request to access his/her information is granted, the person responsible for the records may provide a summary or explanation of protected health information in the designated record set, as long as the individual agrees in advance to this and any associated fees, in lieu of access. The following items should be provided if either (i) the person requests the items, or (ii) the person agrees to our request to provide the items:

- A summary of the requested information instead of or in addition to, providing access to inspect or copy the information.
- An explanation of the protected health information contained in the requested records. This explanation would be delivered to the person when he/she inspects the records, or would accompany the copies of records that are provided to the person.

If a person's request to access his/her information is denied (in whole or in part) for one of the reasons provided in Section D of this policy, the Privacy Officer must provide the person with a summary of the information which the person is not permitted to access.

Duplicate Information: If the same protected health information that is the subject of the request is maintained in more than one designated record set or at more than one location, the agency need only produce the protected health information once in response to the person's request for access. Access need not be provided to records that merely duplicate identical information. However, if a second record provides additional information in any form, that record must be provided.

- ***EXAMPLE***: If a member of the person's planning team makes notations on a laboratory report containing the person's test results, the resulting record will not be considered a duplicate of the original and must also be produced if requested

Collection of Fees: The agency may charge a flat rate fee (not to exceed $6.50), or cost-based fees for labor; for copying and preparation of summaries and explanations; for supplies to provide access in the form and format the individual is requesting; and /or postage for mailing. Procedures for the collection of fees vary depending on the items or services provided.

- Copies - The agency may charge a fee for copies of requested PHI, if it is not already maintained electronically. The Privacy Officer must notify the person (or the person's personal representative) requesting information, in writing, if a fee will be charged, and what the fee will be, and the fee would be collected at the time that the copies are provided.

- Summaries and Explanations - Before preparing or providing a summary or explanation of any Protected Health Information in the designated record set, the person responsible for the records should prepare an estimate of the costs of doing so. The person responsible for the records must notify the Privacy Officer of the estimated costs of preparing the explanation or summary in order for the Privacy Officer to give the person an opportunity to decide whether to continue with the request, modify the request to reduce the costs, or withdraw the request. *Ordinarily, the person must agree to reimburse any estimated costs before the person responsible for the record set will prepare the requested materials.*

  The agency's standard notice of estimated costs of preparing summaries and explanations is maintained by the Privacy Officer, and should be requested by the person responsible for the records upon receiving an individual request for access.

- Supplies and Mailing - The agency may also recover the cost of any postage paid by the agency when mailing materials to the person, or paper or electronic materials used to fulfill the person's request. The **HIPAA Privacy Rights Request** form notifies the person (or person's personal representative) requesting information that the person may be liable for these costs. These fees are collected at the time the copies are provided.

Although the agency may charge for these items and services, a person we support cannot be denied access because of a genuine inability to pay any costs.

3. Recording the Access Provided: If access to protected health information is granted, the Privacy Officer will maintain documentation of the requests and responses in HIPAA compliance files.

D. Denying Access

Reasons for Denial: In the following circumstances, a person's request to access his/her health information should be denied:

(1) The request is not in writing or does not comply with privacy laws;
(2) The information requested is not contained in a designated record set maintained by the agency or any of its business associates;
(3) The request is to inspect or copy psychotherapy notes;
Note: Psychotherapy notes are notes by a mental health professional that (1) document or analyze the contents of a conversation during a private counseling session or during a group, joint, or family counseling session *and* (2) are maintained separately from the person's designated record

set. If a mental health professional's notes are for any reason placed in the person's designated record set, they are no longer psychotherapy notes.

(4) The information was obtained from someone other than a healthcare provider, and (a) the agency agreed to keep the identity of that person confidential, and (b) the person responsible for individual records determines that providing the person with access to the information requested would reveal the identity of that person.

(5) An authorized officer from a correctional institution certifies that granting an inmate's request to *copy* his/her information would (a) jeopardize the health, safety, security, custody, or rehabilitation of that inmate or other inmates, or (b) jeopardize the safety of any other person at the correctional institution, including those who are supervising or transporting inmates. However, the inmate's request to *inspect* his/her information cannot be denied on these grounds. *(65 Fed. Reg at 82555)*

(6) A licensed health care professional (such as a physician, physician's assistant, or nurse) at the agency has determined that granting the person's request is reasonably likely to endanger the *life or physical safety* of the person or another person.

Note: The danger must be to life or physical safety. The request cannot be denied simply because the information is sensitive or has the potential to cause emotional or psychological harm to the person or another person.

(7) The information requested refers to another person, and a licensed health care professional (such as a physician, physician's assistant, or nurse) has determined that granting the person access to this information is reasonably likely to cause substantial harm to that other person. However, access may not be denied if the person who may be harmed is a health care provider.

- ***EXAMPLE:*** A social worker who provides services at the agency has incorporated information about several people in his group therapy notes (other than psychotherapy notes). One of the persons requests access to these notes. The person's request may be denied if the social worker believes that releasing the information contained in those notes is reasonably likely to cause substantial physical, emotional, or psychological harm to one or more of the other people referred to in the notes.

(8) The information was prepared in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding.

(9) The request is made by the individual's personal representative and a licensed health care professional has determined that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

Denial of access for reasons 6, 7, or 9 above, affords the individual the right to have the denial reviewed by a licensed health care professional who did not participate in the original decision to deny.

Partial Denial: If there are grounds to deny the person's access to only part of the protected health information requested, the person responsible for the records, in consultation with the Privacy Officer, will do his/her best to provide the person with access to any other protected health information after excluding the parts the agency cannot let the person inspect or copy. The Privacy Officer may consult with the Corporate Compliance Committee when necessary.

Notice of Denial: If the person's request is being denied, the Privacy Officer must notify the person in writing, within 30 days of receiving the request. The following process should be followed when completing these notices:

- When preparing the denial notice, the Privacy Officer should indicate the grounds for denying the person's access by checking off the appropriate box or boxes on the form provided to the individual.
- If the request is denied because the agency does not maintain the information in a designated record set, the denial notice must state any credible information that the person responsible for the record may have about where the person may obtain access to the requested records.
- If the person's request is only partially denied, the notice must explain what information the person will not be permitted to access and what information the person will be permitted to access.
- If the person has requested an opportunity to inspect records, the notice should include instructions about how they may schedule an appointment to examine the records to which partial access is granted.
- If the person has requested copies of the records, the person responsible for the records in conjunction with Department Director/Vice President or Privacy Officer, should include, along with the partial denial notice, copies of those records to which access is granted (after removing the information which the person is not permitted to access).

Review Process: If access is denied, the person is entitled to challenge or appeal the decision by seeking review according to the following procedures. The denial notice must include a description of how the individual may exercise this right and to whom the person may make a complaint.

First Level of Review The person has a right to a review by a licensed health care professional (designated reviewing official) employed by or contracted with the agency, who was not directly involved in the initial decision to deny the person's request.

- If a person requests this review, the person responsible for the records must transfer the information in dispute to the licensed health care professional. The Privacy Officer is to be kept informed of this transfer. The information in dispute should be accompanied by the denial notice sent to the person (if appropriate) and any further explanation for the reason for denial.

- The designated reviewing official must determine, within a reasonable period of time, whether access was properly denied under any of the grounds provided in Section D of this policy and report the results to the Chief Executive Officer/designee. In most cases, a response should be provided within 10 business days.
- The Chief Executive Officer/designee must notify the person of the results of the review in writing. The agency must take action based on the determination of the designated reviewing official.
- If the designated reviewing official determines through the review process that access should not be granted (in whole or in part), the Chief Executive Officer/ designee will provide a request form which the person may use to challenge or appeal this denial before a committee appointed by the State of New York (see "Second Level of Review" below).

  Second Level of Review If access is denied after the first level of review, the person is entitled to seek a second level of review by the NY State Office for People with Developmental Disabilities (OPWDD) Clinical Record Access Review Committee.
- A person requests this second level of review by writing to the Office of Counsel at OPWDD. The review will be provided at no cost to the person/personal representative.
- If the state review committee decides that the person's request for access should be granted (in whole or in part), the agency must follow the procedures directed by the Committee. The Privacy Officer is to be kept informed of the process.
- If the state review committee decides that the person's request for access was properly denied, the person will be informed by the committee of any opportunity to seek judicial review in the court system (see "Third Level of Review" below).

  Third Level of Review In some cases, the person will be entitled to seek a third level of review by appealing the state review committee's decision to the court system for judicial review. If the Chief Executive Officer designee receives notice that a person has sought judicial review, this notice should be delivered to the agency's Privacy Officer immediately. The Privacy Officer will provide further instruction about whether to resist access in the court system. If the person responsible for the records receives notice, they should refer the committee representative to the Privacy Officer or the Chief Executive Officer/designee. The Privacy Officer will seek guidance from the Compliance Committee and or legal counsel as necessary. The person responsible for the records should not grant access to the person or personal representative unless the Privacy Officer directs the department to do so.

E. Requests for Access by an Individual's Personal Representative

If a person's personal representative requests access to the person's records, the person responsible for the records (in consultation with the Privacy Officer) generally should grant or deny access according to the process in this policy as though the personal representative were the person, *unless one of the following exceptions applies.*

Person Lacking Capacity: When certified that (1) the person lacks the capacity to make health care decisions on his/her own *and* that (2) a personal representative must be given access to the person's information in order to make health care decisions on behalf of the person, the person responsible for the records should grant such access to the personal representative, *even if the person would otherwise be denied access under Section D of this policy*.

Person's Objection: The person responsible for the records, in consultation with a treating physician, should notify any person over the age of twelve (12) years about a personal representative's request for access to his/her information in the following circumstances. If the person objects to access by the personal representative, the person responsible for the records should deny the personal representative's request. The personal representative should be notified in writing of the reason for this denial. *[Note that if the personal representative is the legally designated health care proxy, then s/he has unfettered access to Personal Health Information even if the person objects. The only basis on which to refuse access to the health care proxy is suspicion of some type of abuse (domestic, sexual, etc.) of the person by the health care proxy or that the person would be otherwise endangered.]*

Harm To Person: A personal representative may be denied access to a person's information if a licensed health care professional (such as a physician, physician's assistant, or nurse) has determined that granting such access is reasonably likely to cause substantial harm to the person or a third person. The personal representative should be notified in writing of the reason for this denial and given the opportunity to seek review of the decision as provided in Section D of this policy.

Detrimental Effect from Access by Parent or Legal Guardian: A parent or legal guardian of a minor may be denied access to the minor's protected health information if a treating physician certifies that such access by the parent or legal guardian would have a detrimental effect on: (1) the physician's or the agency's professional relationship with the minor; (2) the care or treatment of the minor; or (3) the minor's relationship with his/her parents or legal guardian. The personal representative should be notified in writing of the reason for this denial and given the opportunity to seek review of the decision as provided in Section D of this policy.

F. Documentation

The Privacy Officer must keep the following documentation in connection with any request by a person or a person's personal representative to access

protected health information. These documents must be maintained by the agency for six years from the date of their creation:

- The request for access, which should be in writing and preferably on the **HIPAA Privacy Rights Request** form;
- Copies of any notice sent to a person or a person's personal representative explaining that the agency requires an extension of time to arrange for the access requested ;
- Copies of any notice sent to a person or a person's personal representative advising that a fee may be charged to recover the costs of providing copies, postage, supplies, and/or summaries or explanations of the information requested;
- Information about any access provided to the person, which should be recorded on the bottom of the **HIPAA Privacy Rights Request** form or other written request;
- A copy of any notice of denial sent to a person or a person's personal representative; and
- A copy of any notice of review results sent to a person or a person's personal representative.

Arc GLOW

Topic: Individual Requests for Additional Privacy Protection	**Ref. No.** 345 – I
Department: Corporate Compliance	**Page:** 1 of 11
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 4/2015, 10/2019, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 5/2016, 4/2017, 4/2018, 6/2023

HIPAA Privacy Regulatory Reference: 45 C.F.R. § 164.522.

PURPOSE

Individuals may request that we provide certain additional privacy protections for their health information. For example, individuals may request restrictions on the way the agency uses and discloses their protected health information for treatment, payment and health care operations. They may also request that we communicate with them by an alternative means or at an alternative location that is more confidential for them. The following policy addresses the procedures that must be followed by the Privacy Officer when handling individual requests for the following types of protections:

- Restrictions on uses and disclosures of protected health information to carry out treatment, payment and health care operations and other uses and disclosures as outlined in Arc GLOW's **Notice of Privacy Practices**
- Confidential communications with the individual or individual's personal representative

POLICY

It is the policy of Arc GLOW to respond to all individual requests with careful consideration and respect. Under the law, special procedures must be followed when handling certain types of requests. All requests for additional privacy protections should therefore be forwarded to the Privacy Officer for careful consideration.

The Privacy Officer or his/her designee(s) should carefully review any individual requests for these privacy protections and determine which requirements below will apply.

Individual requests for privacy protections may only be granted or denied in accordance with the specific requirements below.

The Privacy Officer and his/her designee(s) should be aware that special privacy protections apply to HIV-related information, alcohol and substance abuse information, and some mental health information. Some steps, which are permitted under this policy, may not be permitted when using or disclosing these types of information. The Privacy Officer and his/her designees must also comply with HIPAA Policy #345-F: Privacy of HIV-Related Information and Policy #345-E: Privacy of Psychotherapy Notes, when processing requests involving these sensitive types of information. They are expected to be aware of the requirements under those policies.

To ensure compliance with additional privacy protections approved by the Privacy Officer, all agency personnel affected by this policy are expected to review a person's record for possible restrictions before using or disclosing a person's protected health information.

POSITIONS PRIMARILY AFFECTED

This policy applies to all employees, Board Members, volunteers, interns, contractors, business associates and subcontractors, with primary responsibility of the agency's Privacy Officer and his/her designee(s). References to the Privacy Officer also apply to designee(s).

PROCESS

A. Complying with Additional Privacy Protections

The following process is to be followed by all personnel effected by this policy in response to individual requests for additional privacy protections.

1. Inform the Person

Agency personnel affected by this policy should inform the person that the organization takes his/her requests very seriously and therefore any decision will have to be made by the Privacy Officer, a special administrator within our agency who will appropriately consider his/her specific situation. The individual should be informed that his/her request should be documented on the **HIPAA Privacy Rights Request** form (or a letter with similar information) and will be forwarded to the Privacy Officer for consideration, and that he/she may contact the Privacy Officer if he/she has any questions**.** ***If the person is requesting more***

confidentiality in communications, personnel affected by this policy are <u>not permitted</u> to ask the person's reason for making the request.

2. Refer the Request to the Agency's Privacy Officer

Agency personnel affected by this policy should forward all requests for additional privacy protections to the agency's Privacy Officer, who is the only person authorized to grant or deny the requests. ***Personnel affected by this policy should never grant a person's request, nor provide any assurances that the request will be granted, unless the Privacy Officer, or his/her designee, has specifically approved the request.*** Likewise, the person's request for additional privacy protections should **never be denied outright** by personnel affected by this policy without referring the request to the Privacy Officer. All requests should be treated with respect even if personnel affected by this policy believe that the agency is not likely to agree to the restriction.

3. Notice and Documentation

The Privacy Officer will inform the person of the procedures for submitting a request for additional privacy protection, review the request, and notify the person of the agency's decision. Personnel affected by this policy involved in the person's care will be specifically notified, and the particular privacy protections granted will be documented in the person's record prominently (as determined by the Department Director/ designee) to ensure compliance.

4. Comply with Notices Placing Restrictions on Use and/or Disclosure of Information

Ordinary Circumstances: All Arc GLOW personnel affected by this policy are expected to review a person's record for possible restrictions on the use or disclosure of the person's protected health information. Restrictions will be posted prominently (as determined by the department Director/ designee) in the person's record. *All restrictions must be followed.* Any questions about whether a restriction applies should be directed to the Supervisor, Department Director/Vice President, or the agency's Privacy Officer.

Emergency Circumstances: In rare situations, personnel affected by this policy may ignore a restriction if absolutely necessary to provide the person supported with emergency treatment.

Personnel affected by this policy should attempt to consult with their Supervisors if they believe that a restriction must be ignored in order to provide emergency treatment to a person. If the Supervisor is unavailable, personnel affected by this policy responsible for providing medical treatment may make the decision to ignore the restriction, treat the person and properly document his or her reasons in the person's record. *Other agency personnel affected by this policy should not make these decisions on their own.* If restricted protected health information is disclosed to another health care provider to facilitate the emergency treatment,

the personnel affected by this policy must ask the health care provider not to further use or disclose the information beyond what is necessary to provide the emergency treatment.

B. Terminating Restrictions

The Person's Initiative: A person may request that a restriction be modified or terminated at any time. Where possible, agency personnel affected by this policy should obtain the person's request in writing. If there is insufficient time to obtain a written request, the personnel affected by this policy may accept the person's oral request, which must then be recorded in the person's record as soon as possible. Personnel affected by this policy must send the written request, or documentation of an oral request, to the Privacy Officer/Designee within 3 business days. Only the Privacy Officer/Designee may approve modification or termination of a restriction.

The Agency's Initiative: Arc GLOW may also initiate modification or termination of a restriction at any time, except in the case that the restriction is for disclosures about the individual to a health plan for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual has paid Arc GLOW in full. Any agency personnel affected by this policy who believes there is good reason to modify or terminate a restriction may present his/her reasons to the Privacy Officer for consideration. Only the Privacy Officer may approve modification or termination of a restriction. The termination will only be effective with respect to PHI created or received after Arc GLOW has informed the individual of the termination.

Notice and Documentation: The Privacy Officer will inform the person and personnel affected by this policy of any modifications to, or terminations of, additional privacy restrictions previously granted. The Privacy Officer will also ensure that any modifications and terminations are appropriately documented in the person's record.

C. Complying With Notices Requiring Confidential Communications

Personnel affected by this policy are expected to review a person's record for possible notices requiring that the person be contacted by an alternative method or at alternate locations that are more confidential for the person. These notices will be posted prominently (as determined by the Department Director / designee) in the person's record. Any questions about whether a notice applies should be directed to a Supervisor, Department Director, or the agency's Privacy Officer.

D. Information Specifically for the Privacy Officer

1. Restrictions on Uses and Disclosures of Protected Health Information

Persons supported by the organization have the right to request that we apply further restrictions to the way we use and disclose their protected health information for the following purposes:

- for treatment, payment, or health care operations; and
- to inform family or friends involved in the person's care about the person's condition, or other information relevant to such persons' involvement in the person's care.

The following procedures must be followed when handling these requests.

a. Obtain Request In Writing

All individual requests for these restrictions must be made in writing. The Privacy Officer should encourage the individual supported or the individual's personal representative to complete the request in writing on the **HIPAA Privacy Rights Request** form. Alternatively, the Privacy Officer should encourage the individual or personal representative to write a letter that covers the same information requested on that form.

b. Decision By Privacy Officer

The Privacy Officer must evaluate individual requests for restrictions on a case-by-case basis. The agency is not required to agree to an individual's request, except in the case that the restriction is for disclosures about the individual to a health plan for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual has paid Arc GLOW in full. If it does, it will be bound by its agreement. Factors that should be considered by the Privacy Officer are:

- whether the restriction might cause the agency to violate applicable federal or state law;
- whether the restriction might cause the agency to violate professional standards, including medical ethical standards;
- whether the agency's information systems make it very difficult or impossible to accommodate the restriction;
- whether the restriction might unreasonably impede the agency's ability to provide treatment to the individual;
- whether the individual supported is prepared to make alternative payment arrangements if the restriction will impede the ability of an insurance plan to provide coverage to the individual (for example, if the restriction prevents the agency from disclosing necessary information to the insurer); and

- whether the restriction appears to be in the best interests of the individual supported.

The Privacy Officer must balance these factors to come to a decision. When there is a concern about violating applicable law, the Privacy Officer should consult with the agency's legal counsel. If the Privacy Officer believes that a restriction may be partially accommodated, the Privacy Officer should discuss with the individual whether his/her request can be modified to accommodate the agency's concerns as well as the individual's concerns. This discussion should involve open communication between the Privacy Officer and the individual supported.

c. Notify the Individual Supported

The Privacy Officer must notify the individual supported of the final decision (whether approving or denying the request) in writing. A copy of any notice sent to the individual must also be added to the individual's record.

Granting Request If the Privacy Officer agrees to a restriction, the notice to the individual should state clearly what restriction the agency is agreeing to be bound by. This document should be worded carefully because it will be referred to if any future disputes arise concerning the restriction. However, the notice should also be in language that the individual will understand. Finally, the notice must explain that the restriction will not apply if the individual's information must be used or disclosed to provide the individual with emergency treatment.

Denying Request If the Privacy Officer is denying the request, the notice to the individual supported should state clearly why the agency has decided that it cannot agree to the request. For example, the notice may explain that the agency cannot agree to the restriction because the restriction would cause the agency to violate applicable ethical standards.

d. Notify Agency Personnel affected by this policy and Update Records

If the Privacy Officer agrees to a restriction, he/she will be responsible for communicating the restriction to any other personnel affected by this policy who may be immediately involved in the individual's treatment or billing. The program must document the restriction prominently (as determined by the Department Director / designee) in the individual's record. All personnel affected by this policy are expected to review an individual's record for possible restrictions before using or disclosing any information about the individual for treatment, payment, or healthcare operations or disclosing any information to the individual's family or friends.

e. Notify Business Associates

The Privacy Officer must notify the agency's pertinent business associates about any restrictions agreed to by the agency, as appropriate. The Privacy Officer

should also remind business associates that they are bound by such restrictions under the terms of their contracts with the agency.

f. Effect of Agreement to Restriction

If the Privacy Officer agrees to a restriction, the agency will be bound by this agreement. In most cases, the agency's agreement means that an individual's protected health information may not be used or disclosed in any way that is inconsistent with a restriction placed in the individual's record. However, a few exceptions apply:

Emergency Treatment Exception The agency is not bound by its agreement to a restriction if the individual's protected health information needs to be used or disclosed in order to provide the individual with emergency treatment. Any person to whom protected health information is disclosed for emergency treatment should be instructed not to use or disclose the information other than for the emergency treatment.

Compliance With Other Agency Policies In addition, the agency's agreement to the restriction cannot prevent the agency from using or disclosing an individual's protected health information if that use or disclosure is required in order to comply with U.S. Department of Health and Human Services for the purpose of determining the agency's compliance with HIPAA and to comply with public policy disclosures as required, such as to avert a threat to health and safety or public health activities and risk management.

g. Modifying or Terminating a Restriction

The Privacy Officer may modify or terminate an agreed to restriction only under the following circumstances:

Individual's Initiative An individual may request that a restriction be modified or terminated at any time. The following procedures must be followed when processing an individual's request to modify or terminate a restriction.

- Where possible, the Privacy Officer should obtain an individual's request in writing. If there is insufficient time to obtain a written request, the Privacy Officer may accept the individual's oral request, which must then be recorded in the individual's records as soon as possible.
- If the Privacy Officer agrees to a modification, the Privacy Officer should ensure the modification of all notices of the restriction that are contained in the individual's records.
- If the individual's request is that the restriction be terminated, the Privacy Officer should mark all notices in the individual's records as VOID and note the date the restriction was terminated.

Agency's Initiative The agency may also initiate modification or termination of a restriction at any time, except in the case that the restriction is for disclosures about the individual to a health plan for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual has

paid Arc GLOW in full. The following procedures must be followed to carry out this process.

- Any personnel affected by this policy who believes there is good reason to modify or terminate a restriction may present his/her reasons to the Privacy Officer for consideration. Only the Privacy Officer may approve modification or termination of a restriction.
- If the Privacy Officer approves modification or termination of a restriction, the Privacy Officer must notify the individual supported that the agency wishes to modify or terminate the restriction.
- If the individual agrees to *modify* the restriction, the modified version will apply to all protected health information in the individual's records. If the individual agrees to *terminate* the restriction, the restriction will no longer apply to the individual's protected health information.
- Where possible, the Privacy Officer should obtain the individual's agreement in writing. If there is insufficient time to obtain a written agreement, the Privacy Officer may accept the individual's oral agreement, which *must* then be recorded in the individual's records as soon as possible.
- If the individual agrees to a modification, the Privacy Officer should ensure modification of all notices of the restriction that are contained in the individual's records.
- If the individual agrees to terminate the restriction, the Privacy Officer should mark all notices of the restriction that are contained in the individual's records as VOID and note the date the restriction was terminated.
- If the individual *does not agree* to modify or terminate the restriction, the original restriction will continue to apply to the use and disclosure of any protected health information that was created or received before the date the agency sought to modify or terminate the restriction. The original restriction will not apply, however, to any protected health information that was created or received after the date of termination.
- In this situation, the Privacy Officer should add the following statement to all notices of the restriction that are contained in the individual's records:

> THIS RESTRICTION DOES NOT APPLY TO USES AND DISCLOSURES OF ANY PROTECTED HEALTH INFORMATION THAT WAS CREATED OR RECEIVED ON OR AFTER _____ [INSERT DATE ON WHICH AGENCY SOUGHT TO MODIFY OR TERMINATE THE RESTRICTION].

h. Documentation

The Privacy Officer must maintain the following records to ensure that requests for additional privacy protections are handled properly. These documents must be maintained by the agency for six years from the date of their creation.

- Copies of any individual written requests for restrictions;
- Copies of any notice informing the individual supported about the agency's decision to grant or deny a restriction;
- Copies of any written individual request to terminate a restriction, or alternatively, copies of any documentation in the record that the individual made such a request orally; and
- Copies of any notices of restrictions that have been placed in the individual's record, regardless of whether they were subsequently marked void or partially void.

2. Confidential Communications

Persons supported by our organization have the right to request that we communicate with them about their medical matters in a method or location that is more confidential for them. For example, a person may request that we contact him/her at work instead of at home, or a person may request that we send communications by fax instead of by mail. The following procedures must be followed when handling such requests.

a. Obtain Request in Writing

All individual requests for confidential communications must be made in writing. The individual or the individual's personal representative should be encouraged to complete the request in writing, on the **HIPAA Privacy Rights Request** form. *Neither the Privacy Officer nor any other personnel affected by this policy may ask the individual why he/she is requesting confidential communications. The individual should, however, be asked to provide an alternative address or other method of contact where necessary to comply with the request.*

b. Decision by Privacy Officer

The agency has an obligation to accommodate an individual's request for confidential communications if the agency may reasonably comply with the request. The Privacy Officer must evaluate the reasonableness of an individual's requests on a case-by-case basis. The Privacy Officer may only consider the administrative difficulty of complying with the request. *The Privacy Officer may not refuse to accommodate a request based on his/her perception of the merits of the individual's reason for making the request and may not request or require the individual to provide his/her reason for the request.* Some of the administrative factors the Privacy Officer may consider are:

- whether the alternative method or location of communication might cause the agency to violate applicable federal or state law;
- whether the alternative method or location of communication might cause the agency to violate professional standards, including medical ethical standards;
- whether the agency will be able to communicate with the individual promptly and effectively if it complies with the requested alternative method or location of communication;

- whether the agency will have the ability to apply the alternative method or location of communication consistently;
- whether the alternative method or location of communication would place an unreasonable financial burden on the agency; and
- whether the individual has provided adequate assurances of how payment will be handled if the agency agrees to the alternative method or location of communication.

The Privacy Officer will be required to balance these factors to come to a decision about whether the agency can reasonably comply with the individual's request. When there is a concern about violating applicable law, the Privacy Officer should consult with the agency's legal counsel.

c. Notify the Individual Supported

The Privacy Officer must notify the individual supported of the agency's decision (whether approving or denying the request) in writing where possible. A copy of any notice sent to the individual must also be added to the individual's record.

In some cases, sending a written notice to the individual may be inconsistent with the request for confidential communication. If so, the Privacy Officer may notify the individual orally that the individual's request is being granted and document in the individual's record how the individual was informed.

Granting Request If the Privacy Officer is granting the request, the notice to the individual supported should state clearly how the agency plans to communicate with the individual from that point forward. This document should be worded carefully because it will be referred to if any future disputes arise. However, the notice should also be in language that the individual will understand.

Denying Request If the Privacy Officer is denying the request, the notice to the individual should state clearly why the agency has decided it cannot agree to the alternative method of communication requested. For example, the notice may explain that the agency cannot agree because the agency is concerned that it will not be able to communicate effectively with the individual at the requested location.

d. Notify Agency Personnel affected by this policy and Update Records

If the Privacy Officer agrees that the agency can communicate with the individual through the requested alternative method or at the requested alternative location, the Privacy Officer must ensure the prominent placement (as determined by the Department Director / designee) in the individual's records of a notice explaining how all personnel affected by this policy should communicate with the individual. All personnel affected by this policy are expected to review an individual's records for any notice of confidential communications.

e. Notify Business Associates

If the Privacy Officer agrees to communicate with the individual supported through the requested alternative method or at the requested alternative location, the Privacy Officer must notify the agency's pertinent business associates about this agreement, as appropriate. The Privacy Officer should remind the business associates that, under the terms of their contracts with the agency, they are required to use this alternative method of communication or location if they ever need to contact the individual.

f. Documentation

The Privacy Officer must maintain the following records to ensure that requests for confidential communications are handled properly. These records must be maintained for at least six years from the date of their creation.

- Copies of any individual written requests for confidential communications
- Copies of any notice informing the individual supported about the agency's decision to grant or deny a request for confidential communications.

Arc GLOW

Topic: Individual requests to Amend Protected Health Information (PHI)	**Ref. No.** 345– J
Department: Corporate Compliance	**Page:** 1 of 7
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 2/2014, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 5/2016, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

Individuals generally have a right to request that the agency amend the health information contained in the designated record set that may be used to make decisions about them. The purpose of this policy is to ensure all applicable personnel are aware of their responsibilities to ensure this right.

POLICY

It is the policy of Arc GLOW to treat all individual requests in a respectful manner. To protect the person's privacy, the agency has strict policies and procedures, mandated by state and federal laws, about how and when individual requests for amendment of agency records will be *granted or denied*. Therefore, all individual requests for amendment of records, billing records, or any other records (whether or not they contain individual health information) should be forwarded to the Privacy Officer within 3 business days. *Only the Privacy Officer or other authorized personnel may respond to the individual about his/her request.* Authorized personnel are designated by the agency as the site's Supervisor, Manager, Coordinator, or Director/Vice President. Authorized personnel should notify and work with the Privacy Officer to process such requests in a timely and respectful manner in accordance with the procedures below.

Personnel who are responsible for complying with this policy should be aware that special privacy protections apply to HIV-related information, alcohol and substance abuse information, and some mental health information. Some activities, which are permitted or required under this policy, may not be permitted when using or disclosing these types of information. Personnel subject to this policy must comply with HIPAA Policy #345-F: Privacy of HIV-Related Information and HIPAA Policy #345-E: Privacy of Psychotherapy Notes when processing requests involving these sensitive types of information. Personnel affected by this policy are expected to be aware of the requirements under those

policies. When requests for amendments involve these types of information, personnel affected by this policy should consult the other policies as well.

POSITIONS PRIMARILY AFFECTED

This policy applies to all authorized personnel as described above, with responsibility for individual records, and the Privacy Officer. The policy is also general information that all Arc GLOW employees, interns, volunteers, consultants, contractors, business associates, and subcontractors at the agency should be familiar with.

PROCESSS

A. Right to Request Amendment

What Information: People we support have the right to request that we amend the protected health information that the agency, or one of the agency's business associates, maintains in a "designated record set". A "designated record set" is a group of records that may be used to make decisions about an individual or the treatment or services he/she receives.

The designated record set for each individual generally includes the individual's medical record and billing records.

The specific records included in a designated record set are discussed in HIPAA Policy #345-G: Designated Record Set. Personnel responsible for the record should review that policy in addition to reviewing this policy.

For How Long: Individuals have the right to request amendment of their protected health information for as long as the information is contained in the designated record set.

In Writing: All requests for amendment must be made in writing. Personnel responsible for maintaining the record should encourage the individual or the individual's personal representative to complete the **HIPAA Privacy Rights Request** form or to write a letter that covers the same information requested on that form.

Follow Up Questions: Although an individual's request should be made in writing, authorized personnel are encouraged to follow up on an individual's request in person or by phone if necessary to clarify what information the individual is seeking to amend. Authorized personnel should record on the individual's request form the results of that discussion and initial his/her notes.

B. Response Time

Authorized personnel are expected to respond to individual requests for amendment of their protected health information (by either granting or denying

the request) as soon as possible after the request is received *to ensure satisfaction with our services*.

At the very latest, authorized personnel should respond to the request within 60 days from the date the agency received the request. To ensure that these deadlines are met, the authorized personnel should complete the tracking information at the bottom of the **HIPAA Privacy Rights Request** form. If the person's written request is not made on the form provided, authorized personnel should write in and initial and date the equivalent information on whatever written request was submitted by the person.

- In rare circumstances authorized personnel may be unable to respond within 60 days. If so, the Privacy Officer may extend the time for responding by another 30 days. However, under no circumstances may a response be given later than 90 days from the date the individual's request was received.
- If the 30-day extension is needed, the Privacy Officer must notify the individual in writing within the first 60 days to explain the reason for the delay and the date when the agency expects to answer the individual's request. This notice should be added to the individual's record. The agency's standard notice for this purpose is kept on file by the Privacy Officer.

C. Granting Requested Amendments

A person's request for amendment of protected health information may only be granted according to the following procedures. Authorized personnel must complete these procedures within the time provided in Section B of this policy.

Review of Information: Authorized personnel should determine whether the information that the person would like to amend was created by the agency. They should also determine whether the person would be prohibited from accessing his/her own information under the agency's HIPAA Policy #345-H: Individual Access to Protected Health Information. Arc GLOW cannot amend information that was not created by our agency unless we have reason to believe that the person or organization that did create the information is no longer available to respond to a request for amendment.

Authorized personnel, in consultation with the Privacy Officer, should review the information to determine if an amendment is appropriate. When necessary, authorized personnel should consult with agency personnel who created the information or with other personnel who might be able to verify the accuracy of the information. Authorized personnel should only grant a person's request to amend certain protected health information if he/she determines that the current information is incomplete or inaccurate and should be amended (completely or in part) as requested by the person.

Notify the Individual and Obtain Permission to Notify Others: The Privacy Officer or authorized personnel must notify the person that his/her requested

amendment is being granted, either in whole or in part. The person may be notified in person, by phone, or in writing. When providing notice, authorized personnel should also ask the person the following questions:

- Would the person grant the agency permission to notify other persons or organizations that have relied, or may rely, on the original information in a way that may negatively affect the person?
- Would the person like the agency to notify any other persons that have received the protected health information and would need to know about the amendment?

Make the Amendment: Authorized personnel should make the granted amendment *everywhere* that the specific information to be amended appears in designated record sets maintained by the agency *or its business associates*. The agency's ordinary procedures for correcting the information contained in records should be followed. For example:

- If a document is entirely misplaced and does not belong in the person's record, it may be removed from the record and filed in its proper place.
- If a document belongs in the person's record but contains an error, the author of the record (or authorized personnel if the author is not available) should attempt to make a notation directly on the record that corrects the information *without deleting the original entry*.
- If additional pages are required to correct the information, the authorized personnel should make a notation on the original document directing the reader to the amendment page or pages. Where possible, the amendment page or pages should be physically attached to the original document.
- If the information that needs to be amended is contained in an electronic format, authorized personnel should attempt to make a notation that corrects the information without deleting the original entry, or create a link to a location where the amended information can be found.

Notify Others: Authorized personnel are expected to use all reasonable efforts to forward the amendment to persons or organizations that the person has stated should be notified. If the person agrees, authorized personnel are also expected to notify any person or organization that may have relied, or may rely in the future, on the original information in a way that may negatively affect the person. The person's agreement is not necessary for the agency to notify its business associates.

Future Disclosures: Any future disclosure of the protected health information that has been amended must include the amended information or a link to the amended information. If the information needs to be disclosed through a standard transaction that does not permit inclusion of the additional material required by the amendment, authorized personnel may separately transmit the amended PHI.

D. Denying Requested Amendments

Reasons for Denial: A person's requested amendment may be denied under the following circumstances:

- The request is not in writing;
- The person's request did not explain why he/she believes the agency should make the amendment;
- The information is not contained in a designated record set maintained by the agency or any of its business associates;
- The information was not created by the agency, unless the agency has reason to believe that the person or organization that did create the information is no longer available to fulfill the person's request (for example, if the agency that created the information has closed);
- The person would not be permitted to *access* the information for any of the reasons provided in the agency's policy on Individual Access to Protected Health Information *(*#345-H*)*;
- Authorized personnel have determined that the information is accurate and complete without the requested amendment.

Notice of Denial: If the person's request for an amendment is denied, authorized personnel, in consultation with the Privacy Officer, must notify the person (within 60 days) in writing. The Privacy Officer may consult with the Corporate Compliance Committee, as necessary. The denial notice must include the following:

- The grounds for denying the person's amendment, as noted above in reasons for denial.

  If the grounds for denying the amendment is that the person would not be permitted to access the information, the denial notice must explain the reason that access is not permitted under the agency's policy on Individual Access to Protected Health Information (#345-H*)*.
- If the amendment is only partially denied, the denial notice must explain what portion of the amendment will be granted and what portion will be denied. It must also explain how the person may contact the agency if he/she wishes the agency to make the partial amendment. The partial amendment may not be made without the person's permission. If the person grants permission, authorized personnel must make the partial amendment in accordance with the procedures in Section C of this policy.
- The person's right to request that we include a statement about the amendment and the denial when disclosing the disputed information to other persons in the future, if the individual did not submit a statement of disagreement with the denial.
- The individual's right to submit a written statement disagreeing with the denial and how that individual may file such a statement.

- A description of how the individual may complain to the agency (including name, title and phone number of the Privacy Officer) or to the Secretary of the United States Department of Health and Human Services

Statement of Disagreement: After receiving the agency's denial notice, the person may submit a statement explaining his/her disagreement with our decision. This statement should be limited to two pages.

If the person submits a statement of disagreement, authorized personnel may prepare a written rebuttal statement if necessary to clarify the agency's position about why the amendment should be denied or to respond to issues raised in the person's statement of disagreement. A copy of this rebuttal statement must be provided to the person.

Record Keeping: Authorized personnel must physically attach, or electronically link, the following documents to the protected health information in the designated record set that was the subject of the disputed amendment (in every place that the information appears in the person's designated record sets):

- the person's written amendment request;
- the agency's notice denying that amendment request;
- the person's statement of disagreement (if any); and
- the agency's rebuttal statement (if any).

Future Disclosures: Certain documents must be included in any future disclosure of the person's protected health information, as discussed below. If the person's protected health information needs to be disclosed through a standard transaction that does not permit inclusion of the materials required below, authorized personnel may separately transmit these materials.

Statement of Disagreement If the person has submitted a statement of disagreement, authorized personnel must include the following documents in any future disclosure of the protected health information that is the subject of the dispute:

- the person's written amendment request;
- the agency's notice denying that amendment request;
- the person's statement of disagreement; and
- the agency's rebuttal statement (if any).

An accurate summary of the denial notice, the person's statement of disagreement, and the agency's rebuttal statement may be included in lieu of the original documents. *The person's amendment request must always be included in its entirety.*

No Statement of Disagreement If the person does not submit a statement of disagreement, the person's amendment request and the agency's denial notice should be included in any future disclosures of the protected health information that is the subject of the amendment request *only if the individual has requested such action.*

E. Compliance with Amendments Reported From Other Organizations

If another organization informs the agency that it has granted a person's request to amend his/her protected health information (and how that information has been amended) authorized personnel must amend that person's protected health information *everywhere* it appears in the designated record set maintained by the agency. These amendments should be made in accordance with the procedures set forth in Section C of this policy, including notifying the person and others (where appropriate) that the amendment has been made.

Arc GLOW

Topic: Individual Authorizations for Release of Protected Health Information	**Ref. No.** 345- K
Department: Corporate Compliance	**Page:** 1 of 2
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 2/23/22	**Revised:** 1/2014, 10/2019, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 5/2016, 4/2017, 4/2018, 6/2023

PURPOSE

The purpose of this policy is to ensure all applicable personnel understand their responsibility to obtain authorization from the people we support for uses and disclosures of protected health information for purposes other than treatment, payment, and health care operations and other permissible uses as outlined in Arc GLOW's **Notice of Privacy Practices.**

POLICY

Arc GLOW is committed to protecting the privacy and confidentiality of health information about the people we support. It is the responsibility of every person affected by this policy to preserve the privacy and confidentiality of protected health information of people supported by Arc GLOW. All personnel affected by this policy are expected to demonstrate this commitment by following the processes below for obtaining authorization to release information for all disclosures that are not for treatment, payment, and health care operations, or other permissible uses as outlined in Arc GLOW's **Notice of Privacy Practices**.

POSITIONS PRIMARILY AFFECTED

This policy applies to all Arc of Livingston-Wyoming personnel, which includes all employees, interns, volunteers, consultants, contractors, business associates and subcontractors of our organization.

PROCESS

A. An **Individual Authorization to Release Protected Health Information** form must be completed to release information that is for any purpose other than treatment, payment, or health care operations, or that is not to: the individual or their personal representative; persons involved in the individual's care;

business associates in their legitimate duties; or not for public purposes and other permissible uses as outlined in the **Notice of Privacy Practices**.

B. The personnel affected by this policy providing the information to others must complete the “Use and Disclosure Covered by this Authorization” section of the **Individual Authorization to Release Protected Health Information (PHI)** form before obtaining a signature from the authorized person.

C. The signature and contact information of the person supported or their personal representative who is granting authorization must be obtained.

D. The person supported by Arc GLOW has the right to see and obtain a copy of the information described on the authorization form and a copy of the **Individual Authorization to Release PHI** form. If he/she requests to see the information or to receive a copy of the information, the person responsible ensures that his/her request is granted.

E. The **Individual Authorization to Release PHI** form is maintained in the person’s file by the person responsible for the records, and is not valid after its expiration date (which cannot exceed 1 year).

Arc GLOW

Topic: General Policy for Accountings of Disclosures	**Ref. No.** 345 – L
Department: Corporate Compliance	**Page:** 1 of 3
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 3/2014, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 5/2016, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

People supported by Arc GLOW have a right to an "accounting of disclosures", which is a list of certain types of disclosures of the person's protected health information that the agency has made to third parties in the six years prior to the date of the request. The purpose of this policy is to ensure that all requests for accounting of disclosures are made and responded to in accordance with HIPAA privacy regulations.

POLICY

It is the agency's policy to treat all requests for accounting of disclosures in a respectful manner. Arc GLOW will track all disclosures that may need to be included in any future accounting lists requested by a person supported. A person supported may request an accounting list at any time. Agency designated employees must therefore "track" all disclosures of information that could possibly be needed to respond to a person's future request. Disclosures are tracked by recording information about the disclosures as outlined in the **PHI Use and Disclosure Inventory Log.** While the employee responsible for individual records will often be responsible for making disclosures and tracking their own disclosures, other designated agency employees may also make disclosures. This process therefore will require the diligent participation of all agency employees. Any agency employee who discloses an individual's protected health information MUST complete a tracking form, unless an exception applies in accordance with Process A below. Completed tracking forms are to be maintained in the individual's permanent record.

Each and every agency personnel responsible for protected health information will be expected to comply with this policy of tracking disclosures. Seemingly minor violations (such as skipping information required on forms) will be subject

to serious disciplinary action because of the potential harm that may be caused if accurate information cannot be recovered when the individual requests it.

POSITIONS PRIMARILY RESPONSIBLE

This policy applies to all agency employees, interns, consultants, contractors, or business associates that are responsible for protected health information.

PROCESS

All requests made by a person supported for accounting lists should be forwarded to the agency's Privacy Officer/Designee within three business days. Designated Supervisors, Directors/Vice Presidents, and the Privacy Officer are the authorized employees responsible for preparing the accounting list and responding to a person's request.

A. Types of Disclosures Which Must Be Tracked

Agency designated employees must track all disclosures of an individual's protected health information made by the agency or its business associates to a third party, *except for:*

- Disclosures for treatment, payment or health care operations
- Disclosures made to the individual or the individual's personal representative (parent, legal guardian, spouse, adult child, health care agent) involved in the person's care
- Disclosures made to others with an authorization to release the information
- Disclosures made for national security or intelligence purposes
- Disclosures made to correctional institutions or law enforcement officials for certain purposes regarding individuals or inmates in lawful custody
- Disclosures made as part of a limited data set (PHI which excludes any identifying information, and is used only for purposes of research, public health or health care operations in accordance with a Data Use Agreement)
- Disclosures that occurred prior to April 14, 2003

B. Information Required For Each Disclosure

The following information must be included for each disclosure on the **PHI Use and Disclosure Inventory Log** form:

- The date of the disclosure;
- The name of the person or organization that received the protected health information;
- The address of the person or organization that received the information (if known);
- A brief description of the protected health information disclosed (with dates of treatment when possible); AND at least one of the following:
    - A brief statement explaining the purpose of the disclosure and the basis on which the disclosure was permitted under our agency's policies,

- A copy of the individual's authorization form permitting the disclosure
- A copy of a written request made by a person or organization to whom disclosure was made where the information was disclosed for public policy purposes, in accordance with 45 CFR 164.512, or for purposes of compliance investigations by the Secretary of Health and Human Services (attach to form).

EXCEPTION: If a series of disclosures is made to the same government entity for the same purpose, agency employees need only include the information above for the *first* disclosure made during the accounting period where the disclosure is made, the frequency or number of disclosures made during the accounting period to that entity, and the date of the last such disclosure during the accounting period.

Arc GLOW does not routinely disclose protected health information for research purposes. Should this occur, accounting of disclosures shall be documented with guidance from the HIPAA Privacy Officer, in accordance with 45 CFR 164.528 (b)(4) and Policy #345-M : Accounting of Disclosures for Employees Responsible for Individual Records .

Arc GLOW

Topic: Accounting of Disclosures for Employees Responsible for Individual Records	**Ref. No.** 345 – M
Department: Corporate Compliance	**Page:** 1 of 6
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 3/2014, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 11/12, 4/2015, 5/2016, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

People supported by Arc GLOW have a right to an "accounting of disclosures," which is a list of certain types of disclosures of the individual's protected health information that the agency has made to third parties in the six years prior to the date of the request. The purpose of this policy is to ensure that designated personnel receive and process requests for accounting of disclosures in accordance with HIPAA privacy regulations.

POLICY

It is Arc GLOW's policy to treat all individual requests in a respectful manner. Employees responsible for individual records are therefore expected to track all disclosures that may need to be included in any future accounting lists requested by individuals, in accordance with Policy #345-L: General Policy for Accounting of Disclosures, on the agency's **PHI Use and Disclosure Inventory Log.**

Authorized employees responsible for maintaining the individual records are expected to respond to individual requests for accounting lists in a timely and respectful manner in accordance with the process below.

Employees responsible for complying with this policy should be aware that special privacy protections apply to HIV-related information, alcohol and substance abuse information, and some mental health information. Some activities, which are permitted under this policy, may not be permitted when using or disclosing these types of information. Employees must comply with HIPAA Policy: Privacy of HIV-Related Information (#345-F) and Privacy of Psychotherapy Notes (#345-E) when processing requests involving these sensitive types of information. They are expected to be aware of the requirements under those policies.

POSITIONS PRIMARILY RESPONSIBLE

This policy applies to designated Supervisors, Directors/Vice Presidents, and the Privacy Officer, who are the authorized employees responsible for individual records and/or receiving and processing requests for accounting of disclosures. Other designated individuals shall be determined by the Privacy Officer or Department Director/Vice President as necessary.

PROCESS

Employees responsible for individual records should respond to individual requests for accounting of disclosures in accordance with the following process. All individual requests for accounting lists should be forwarded to the Privacy Officer/Designee within three business days. The Privacy Officer/Designee will contact the designated employee responsible for the individual's records and will review the **PHI Use and Disclosure Inventory Log** to verify that it has been completed in accordance with this policy and Policy #345-L: General Policy for Accounting of Disclosures.

A. Receipt of Individual Requests

In Writing: All individual requests for accountings of disclosures must be made in writing. Employees responsible for individual records are to encourage the individual or the individual's personal representative to complete the **Request for Accounting of Disclosures of Protected Health Information.** Alternatively, employees should encourage the individual to write a letter that covers the same information requested on that form.

Follow Up Questions: Although an individual's request must be made in writing, employees are encouraged to follow up on an individual's request in person or by phone if necessary to clarify the accounting list the individual is seeking to have prepared. The employee responsible for the individual's record should record on the individual's request form the results of that discussion and initial his/her notes.

B. Response Time Requirements

Employees responsible for individual records, upon approval from the Privacy Officer, are expected to provide the individual with the requested accounting list as soon as possible. At the very minimum, employees responsible for the individual's record must provide the list within 60 days from the date the agency received the request.

In rare circumstances, Arc GLOW may be unable to provide the accounting list within 60 days. If so, the Privacy Officer may extend the time for responding by another 30 days. However, under no circumstances may the agency provide the list later than 90 days from the date the individual's request was received.

If the 30-day extension is needed, the Privacy Officer will notify the individual in writing within the first 60 days to explain the reason for the delay and the date when the agency expects to provide the accounting list. A copy of the agency's standard notice letter for this purpose will be kept on file by the Privacy Officer.

C. Content of the Accounting List

Employees responsible for individual records are to prepare the content of an accounting list as follows.

1. Determine Period of Accounting: Employees responsible for the individual's record are to first determine the period of accounting which will be covered in the accounting list. Individuals may request an accounting of disclosures made during any period of time falling within six years before the date of the request.

2. Collect Tracking Forms: Because an individual may request an accounting list at any time, agency employees are expected to track all disclosures which may need to be included in any future accounting lists requested by individuals. For more information about what disclosures must be tracked, see the General Policy for Accountings of Disclosures (#345-L). When preparing an accounting list, employees responsible for individual records should collect all **PHI Use and Disclosure Inventory Logs** in departments throughout the agency that tracked disclosures of the individual's protected health information *during the period of accounting requested by the individual* UNLESS the disclosures tracked on the form were made for one of the following purposes:

- Disclosures made pursuant to the individual's specific authorization;
- Disclosures made to individuals or entities outside the agency where necessary for the agency or the recipient to provide treatment to individuals, obtain payment for that treatment, or carry out the routine business operations that qualify as health care operations;
- Disclosures of individual information that are made in accordance with the agency's policy on Individual Access to Protected Health Information (#345-H);
- Disclosures made to the individual's friends and family involved in the individual's care or payment for the individual's care;
- Disclosures of a limited data set pursuant to a data use agreement;
- Disclosures made for national security and intelligence purposes;
- Disclosures made about inmates to correctional institutions or law enforcement officials; and
- Disclosures made before April 14, 2003.

3. Include Information Required for Each Disclosure in the Accounting: When preparing an accounting list, the following information must be included for each disclosure on the **PHI Use and Disclosure Inventory Log** that has been collected in accordance with the procedure above:

- The date of the disclosure;
- The name of the person or organization that received the information;

- The address of the person or organization that received the information (if known);
- A brief description of the protected health information disclosed (with dates of treatment when possible); and at least one of the following:
  - A brief statement explaining the purpose of the disclosure and the basis on which the disclosure was permitted under our agency's policies
  - A copy of the individual's authorization form permitting the disclosure
  - A copy of a written request made by a person or organization to whom disclosure was made where the information was disclosed for public policy purposes, in accordance with 45 CFR 164.512, or for purposes of compliance investigations by the Secretary of Health and Human Services (attach to form).

EXCEPTIONS:

***Series of Disclosures*:** If a series of disclosures was made to the same person or organization for the same purpose or on the basis of a single authorization form, employees responsible for individual records need only include the information above for the *first* disclosure made during the accounting period. The accounting must then provide the following information to cover the rest of the series:

- Frequency, periodicity, or number of disclosures made in the series
  - EXAMPLE: Disclosures were made every 2 months.
  - EXAMPLE: A total of 15 disclosures were made during the accounting period.
- The date of the last disclosure in the series that was made during the accounting period.

Employees responsible for individual records may also use this abbreviated procedure to account for a series of disclosures that was made for a *single purpose* permitted in public policy.

Disclosures for Certain Research Activities: Abbreviated procedures apply for disclosures of an individual's protected health information in the course of certain research activities for which:

- The agency's Privacy Officer has approved (in accordance with agency policy and 45 CFR164.512(i)) disclosure of protected health information about individuals enrolled in the study without their written authorization; and
- The research study involves disclosures of protected health information for 50 or more individuals.

The Privacy Officer will maintain a list of such research activities. Employees responsible for individual records should consult with the Privacy Officer to determine whether the individual's information has been used or disclosed for

one or more of these research activities. If so, employees responsible for the individual records should obtain from the Privacy Officer and include in the individual's accounting list a properly completed **Accounting of Disclosures for Research Activities** form for each research activity. After reviewing the accounting list provided, if an individual requests further information about how to contact the researchers to whom it is likely the individual's information was disclosed, employees responsible for the individual records should refer the individual's request to the agency's Privacy Officer.

4. Follow-up on Gaps in Information: Employees responsible for individual records should follow-up with other agency employees to fill in any gaps in required information. They should also report to the Privacy Officer any significant failure of agency employees to appropriately track disclosures needed to provide accounting lists in accordance with this policy.

D. Exclusion at Government Request

In some cases, a health oversight agency or law enforcement official may request that the agency temporarily suspend an individual's right to receive an accounting of the disclosures made to that agency or official. The following procedures must be followed before honoring such a request.

Written Request: The agency or official must present to Arc GLOW a statement, in writing, that providing the individual with an accounting of disclosures made to the agency or official would be "reasonably likely to impede the agency or official's activities." This statement must also specify how long the suspension will be required.

- During the period of suspension, employees responsible for individual records must prepare the accounting list requested by the individual but exclude any disclosures that were made to the agency or official. *Do not notify the individual that these disclosures were excluded.*
- When the suspension period is over, employees responsible for individual records must include the disclosures made to the agency or official in any accounting for the individual.

Oral Request: If the agency or official asserts that there is insufficient time to prepare a written statement, the Privacy Officer may grant a suspension for 30 days based on the agency or official's oral representation that suspension is needed for the reasons above (in person or on the telephone).

- An employee responsible for individual records must document that these statements were made by the agency or official in person or on the phone. The employee must also record the identity of the agency or the official.
- After 30 days, the employee responsible for the individual record must include the disclosures made to the agency or official in any accounting for the individual unless the agency or official has provided a written statement seeking further suspension. The agency's or official's written statement must meet the

requirements explained above about why the suspension is necessary and how long it will last.

E. Collection of Fees

Individuals are entitled to obtain from Arc GLOW one free accounting list every 12 months. If an individual requests any additional accounting lists within the same 12-month period, the Privacy Officer may prepare an estimate of a reasonable fee that will recover the costs of producing those lists. The Privacy Officer will notify the individual, in writing, of this estimated fee and give the individual an opportunity to decide whether to continue with the request, modify the request to reduce the fee, or withdraw the request. *The individual's permission to move forward with preparing the list is required any time a fee will be charged to recover the costs of fulfilling the request.* Permission may be oral or written, as long as the permission is documented in the individual's records. A copy of the agency's standard notice of potential fees will be kept on file by the Privacy Officer.

F. Documentation

Employees responsible for individual records must maintain the following records to ensure that the agency properly responds to requests for accountings of disclosures. These documents must be maintained by the agency for six years from the date of their creation.

- Completed **PHI Use and Disclosure Inventory Log** forms for all disclosures that may possibly need to be included in a future accounting list for the individual;
- Copies of any requests by the individual for accounting lists (which must be in writing and preferably on **Request for Accounting of Disclosures of Protected Health Information** form);
- Copies of any notices to the individual explaining that the agency requires an extension of time to prepare the requested accounting list;
- Copies of any notices to the individual advising that a fee may be charged for providing an accounting list or lists; and
- Copies of any accounting lists provided to the individual.

Arc GLOW

Topic: Fundraising Activities	**Ref. No.** 345 – N
Department: Corporate Compliance	**Page:** 1 of 4
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 3/2014, 4/2015, 4/2017, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 12/11, 5/2016, 4/2018, 10/2019, 6/2023

PURPOSE

The purpose of this policy is to define the position of Arc GLOW in relationship to fundraising and protected health information.

POLICY

Arc GLOW does not generally disclose protected health information for the purposes of fundraising. If it is determined that this may be necessary, fundraising activities involving the use or disclosure of individual protected health information may only be conducted after being approved by the Director of Public Relations and Development/designee and Privacy Officer, who will ensure that all requirements for the use and disclosure of individual protected health information have been met. Individual information or lists should not be used or released before this approval has been obtained.

POSITIONS PRIMARILY AFFECTED

This policy applies to all agency employees, interns, volunteers, consultants, contractors, and subcontractors. Personnel affected by this policy that are authorized to conduct fundraising activities involving the use or disclosure of individual protected health information should pay special attention to Section B.

PROCESS

A. Fundraising Activities Subject To This Policy

Fundraising activities include any activities undertaken to raise money or other things of value on behalf of our organization or another organization. The activities may be undertaken by the organization (including agency volunteers), business associates, or other bodies, which may have a vested interest in assisting Arc GLOW.

Examples of fundraising activities include:

- Requests for general donations to benefit the agency;

- Requests for special-purpose donations (for example, to benefit autism research or to remodel a reception area);
- Requests for sponsorship of agency events or activities (for example, a charity dinner, golf tournament); and
- Auctions, rummage sales, or bake sales.

The fundraising activities are subject to this policy only if the activities involve the use or disclosure of a person's protected health information. Examples: Donation requests directed to people previously supported by Arc GLOW would involve the use of protected health information while rummage sales conducted by agency volunteers and open to the general public (and for which invitations have not been sent or given to people supported) would not.

B. "Opt-Out" Option

Everyone has the right to opt out of receiving certain types of fundraising communications. All requests to opt out of such communications, or any **Fundraising Opt-Out** Forms, should be forwarded to the Public Relations Director by the personnel authorized to conduct fundraising activities.

A **Fundraising Opt-Out** form / statement accompanies any written fundraising materials that are mailed or distributed. Any forms or opt-out requests received by anyone other than the Public Relations Director/designee are to be forwarded to the Director of Public Relations and Development/designee**,** who will then be responsible for ensuring the removal of the person's name from any future mailing lists and adding a copy of the **Fundraising Opt-Out** form/request to the record. Every reasonable effort should be made to ensure that the person who opts out of receiving further fundraising communications is not sent such communications.

Failure to adhere strictly to a person's request to opt-out of fundraising solicitations not only will damage the organization's reputation and relationship with others but also could subject the agency to penalties and claims under applicable federal and state law.

Additional Requirements for Consideration by Personnel Authorized to Conduct Fundraising Activities

Personnel responsible for complying with this policy should be aware that special privacy protections apply to HIV-related information, alcohol and substance abuse treatment information, and mental health information. Some activities, which are permitted under this policy, may not be permitted when using or disclosing these types of information. Personnel authorized to conduct fundraising activities must comply with HIPAA Policy: Privacy of HIV-Related Information (#345-F) and the policy on Privacy of Psychotherapy Notes (#345-E), when using or disclosing these

sensitive types of information for any reason. They are expected to be aware of the requirements under those policies.

The personnel authorized to conduct fundraising activities must work with the Director of Public Relations and Development and Privacy Officer to determine which type of fundraising activity is occurring, to ensure all applicable privacy protections required have been met.

C. Fundraising Not Requiring Individual Authorization

Authorized personnel affected by this policy may use or disclose to a **business associate or an institutionally related foundation**, the following *limited* information without written authorization from the individual, to raise funds or solicit donations for the benefit of the agency:

- individual name;
- address and other contact information;
- age;
- gender;
- date of birth;
- insurance status; and
- dates of service provided by the agency by department.

D. Fundraising Requiring Individual Authorization

Any other use or disclosure of an individual's protected health information for fundraising purposes requires the individual's authorization. An authorization is therefore necessary if:

- additional individual information is used or disclosed;
- individual information is used by or disclosed to individuals or entities <u>other than</u> Arc GLOW personnel affected by this policy or business associates undertaking fundraising activities for our agency; or
- the purpose of the fundraising effort is to raise money or other things of value for the benefit of an organization other than Arc GLOW.

For example, personnel authorized to conduct fundraising activities must obtain an individual's authorization before using the individual's protected health information to solicit funds from individuals for or on behalf of an outside nonprofit organization that engages in research, education, and awareness efforts about a particular disease. All individual authorizations completed for the purpose of fundraising activities must be forwarded to the Director of Public Relations and Development or the Privacy Officer.

E. Recording Any And All Disclosures

The Public Relations Office, in coordination with the Privacy Officer, maintains a central file of the signed individual authorizations for fundraising activities involving the use and disclosure of protected health information. The Public Relations Office records any and all disclosures of an individual's protected health information that are made to persons other than agency employees or the individual who is the subject of the information when conducting fundraising activities. The Public Relations Office should record disclosures made for fundraising purposes on the **PHI Use and Disclosure Inventory Log,** in accordance with HIPAA General Policy for Accounting of Disclosures (#345-L). Failure to record properly a disclosure of an individual's protected health information made for fundraising purposes when required will be treated as a violation of this policy.

Arc GLOW

Topic: Use and Disclosure of Protected Health Information for Marketing Activities	**Ref. No.** 345 – O
Department: Corporate Compliance	**Page:** 1of 3
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved: 12/10, 12/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 3/2014, 4/2015, 1/2022
Responsible Director: Corporate Compliance	**Reviewed:** 11/11, 12/11, 5/2016, 4/2017, 4/2018, 10/2019, 6/2023

PURPOSE

The purpose of this policy is to ensure that marketing activities involving disclosure of protected health information are conducted in accordance with the federal HIPAA privacy regulations.

STATEMENT OF POLICY

Arc GLOW permits marketing activities that are sensitive to the needs of people we support and consistent with our mission. Arc GLOW will carefully evaluate the agency's participation in any marketing of our services, as well as any marketing proposed to be undertaken by third parties. Most marketing communications involving the use of protected health information about people we support cannot be made without first obtaining the person's written authorization. Proposed marketing activities therefore must be examined to determine whether such authorization will be required.

Arc GLOW marketing activities involving the use or disclosure of protected health information may only be conducted after being approved by the Director of Public Relations and Development, who will work with the Privacy Officer to ensure that all requirements for the use and disclosure of protected information have been met. No information or list containing information about people we support should be used or released before this approval has been obtained. Proposed marketing activities may only be approved if all applicable requirements for the use and disclosure of protected information (as set forth below) have been met.

Marketing employees are employees authorized by the Public Relations Department or Chief Executive Officer to conduct marketing activities and are responsible for complying with this policy. These employees should be aware

that special privacy protections apply to HIV-related information, alcohol and substance abuse treatment information, and mental health information. Some activities that are permitted under this policy may not be permitted when using or disclosing these types of information. Marketing employees must comply with HIPAA Policy: Privacy of HIV-Related Information (#345- F) and HIPAA Policy: Privacy of Psychotherapy Notes (#345-E) when using or disclosing protected health information, or approving marketing activities involving the use or disclosure of these sensitive types of information for any reason. Employees responsible for marketing activities are expected to be aware of and abide by the requirements of those policies.

POSITIONS PRIMARILY AFFECTED

General information contained in this policy applies to all Arc GLOW employees, interns, volunteers, consultants, contractors, and subcontractors at the agency.

Specific information in this policy applies to the Privacy Officer, Public Relations personnel, and all authorized employees conducting or approving marketing activities involving the use or disclosure of individual protected health information. Such employees are referred to in this policy as "marketing employees."

PROCESS

A. Marketing Activities Subject To This Policy

Marketing activities generally include all oral or written communications with a person about a product or service that encourages the person to purchase or use that product or service. Agency marketing activities may involve the use or disclosure of a person's protected health information because the marketing is directed at people who are currently receiving or who previously received services from the agency. Marketing also includes distributing protected health information about the people we support to another organization so that that organization may market its own products and services if the agency receives direct or indirect remuneration for providing the organization with this protected health information.

This policy generally *does not* apply to various activities related to the routine treatment or routine operations of the agency, *even if* those activities involve the use or disclosure of protected health information to communicate with people concerning products or services. Examples of activities that *do not* constitute marketing include:

1. telling people whether a product or service is provided by the agency;
2. indicating whether a product or service will be covered by insurance;
3. discussing products or services that may further a particular person's treatment;

4. describing potentially beneficial products or services in the course of managing or coordinating a particular person's care or treatment; or
5. recommending alternative treatments, therapies, health care providers, or settings of care.

B. Marketing Activities That Do Not Require Authorization

A person's written authorization is ***not*** required to use and/or disclose his/her protected health information in connection with the following marketing communications made directly to the person:

- Communications that occur face-to-face (including giving the person a product sample), or
- Communications involving a promotional gift of nominal value (including giving a person pens, calendars, or other merchandise) that generally promotes the agency.

C. Marketing Activities That Require Authorization

For *all other types of marketing communications*, a person's protected health information may only be used or disclosed if the person signs a written authorization for the communication by completing the **Individual Authorization to Release PHI** form. Examples of marketing communications that require written authorization include:

- Sending a person a brochure endorsing the use of another organization's products or services when those products or services are not necessary for that specific person's course of treatment (for example, a mass mailing to all individuals of brochures generally promoting the products and services of a home health agency), and
- Disclosing personal information to third parties, in exchange for direct or indirect remuneration, so that such third parties may use the information for their own marketing activities (for example, selling people's names to pharmaceutical manufacturers for them to use in drug promotions).

The person's written authorization is required even if the agency intends to use an outside vendor or business associate to make the marketing communication on behalf of the agency. Marketing employees authorized to conduct marketing activities must obtain an individual's written authorization before using the individual's protected health information. All individual authorizations completed for the purpose of marketing must be forwarded to the Public Relations Office or the Privacy Officer.

D. Accounting for Disclosures

The Director of Public Relations and Development/designee, in coordination with the Privacy Officer, accesses central/individual files to ensure there is a signed individual authorization for any marketing activities involving the use and disclosure of protected health information. The Public Relations Office should ensure that all disclosures of protected health information in connection with marketing activities are recorded when and as required by the agency's HIPAA General Policy for Accounting of Disclosures (#345-L).

Arc GLOW

Topic: Business Associate Agreements	**Ref. No.** 345 – P
Department: Corporate Compliance	**Page:** 1 of 4
Function: HIPAA Privacy Compliance	**Originated:** 12/2010, 1/2022 (as Arc GLOW)
Board Approved:12/10, 1/11, 12/12, 5/2014, 5/2015, 5/2016, 4/2017, 4/2018, 1/22/2020, 3/23/22	**Revised:** 3/2014, 1/2022, 6/2023
Responsible Director: Corporate Compliance	**Reviewed:**11/11, 11/12, 4/2015, 5/2016, 4/2017, 4/2018, 10/2019

PURPOSE

The Health Insurance Portability and Accountability Act Privacy Regulations require that a covered entity (Arc GLOW) obtain and document satisfactory assurances from its business associates (those persons or entities permitted to create, receive, maintain or transmit protected health information on behalf of Arc GLOW, who do not act as employees of the agency) that the business associate will appropriately safeguard all protected health information (PHI).These business associates must also obtain satisfactory assurances that any subcontractors will safeguard all of Arc GLOW's protected health information. The purpose of this policy is to ensure compliance with this regulation.

POLICY

Arc GLOW strives to protect the confidentiality, integrity, and availability of PHI by permitting a business associate to create, receive, maintain, or transmit PHI on its behalf only if there is a written agreement between Arc GLOW and the business associate that provides assurances that the business associate will appropriately safeguard such PHI. Business associates also must obtain satisfactory assurances in the form of a business associate agreement from subcontractors that the subcontractors will safeguard any of Arc GLOW's PHI in their possession.

A **Business Associate Agreement** is required when Protected Health Information is being shared between Arc GLOW and its business associates. Protected Health Information is individually identifiable health information that is transmitted or maintained in electronic or any other form or medium. Individually identifiable health information is related to the past, present, or future physical or

mental health or condition of an individual; the provision of medical care to the individual; or the payment for such care that identifies or may be used to identify the individual, which is created or received by a Covered Entity, regardless of when or how it was created or obtained.

A **Business Associate Agreement** is to be attached to all Arc GLOW contracts in which the business associate has persistent custody of and access to Protected Health Information which may be used or disclosed.

Examples of business associates may include: computer consultants, accounting/auditing services, billing and coding services, shredding services, systems vendors who access PHI, technical support services that may access PHI (software, fax/ copiers, etc.), and legal consultants.

Examples of those who are not business associates are tradesmen /construction contractors, housekeeping services, or office supply vendor.

The **Business Associate Agreement** requires the business associate to:

- Appropriately safeguard all protected health information, in accordance with the **Business Associate Agreement** and HIPAA privacy regulations, or as required by law;
- Report to Arc GLOW any misuse of protected health information, including breaches of unsecured PHI;
- Secure satisfactory assurances from any subcontractor that they will safeguard the PHI;
- Grant individuals access and ability to amend their private health information;
- Make available an accounting of disclosures;
- Release applicable records to the Dept. of Health and Human Services Secretary, if requested; and
- Upon termination of the contract / **Business Associate Agreement,** return or destroy all protected health information received from, or created and received by the business associate on behalf of Arc GLOW.

The contract or other written arrangement must authorize termination if the business associate violates the terms of the contract or **Business Associate Agreement.**

If the covered entity and business associate are both governmental entities, a memorandum of understanding may provide satisfactory assurances. Other laws, such as adopted regulations or a subpoena, may also provide assurances. In each case the above requirements must be met.

When the business associate is required by law to perform a function or activity on behalf of Arc GLOW, Arc GLOW may disclose PHI to the business associate to the extent necessary to comply with the legal mandate and no written agreement need be executed. However, Arc GLOW must attempt in good faith to obtain satisfactory assurances and document any attempts and reasons they could not be obtained.

POSITIONS PRIMARILY AFFECTED

All agency employees should have an understanding of the requirements of this policy, but the positions primarily affected are those members who are representatives of the Compliance, those who initiate contracts, and the Privacy Officer/designee.

PROCESS

A. Business Associates of Arc GLOW

1. The Vice President of Compliance, in conjunction with the Privacy Officer, will oversee all **Business Associate Agreements.** Prior to allowing a business associate to access PHI or Electronic PHI, the Privacy Officer/designee must be contacted to generate a business associate agreement.
2. The Vice President of Compliance, in conjunction with the Privacy Officer will retain an approved agency **Business Associate Agreement** template and will generate a specific business associate agreement.
3. The Vice President of Compliance, in conjunction with the Privacy Officer will submit the prepared **Business Associate Agreement** and any other required documentation to the Chief Executive Officer/Designee for review and approval prior to the agreement being sent to the identified business associate.
4. The signed, returned **Business Associate Agreement** will be maintained electronically. A copy may be maintained by the designated Program Director. The business associate will not be allowed access to PHI or EPHI until the signed agreement has been received.

B. Arc GLOW as a Business Associate of Another

Covered Entity

1. All **Business Associate Agreements** generated by organizations with which we do business, shall be forwarded to the agency's Vice President of Compliance.
2. The Vice President of Compliance, in conjunction with the Privacy Officer will review the agreement, recommend any changes to ensure compliance with applicable regulations and laws, and submit the **Business Associate Agreement** to the Chief Executive Officer / Designee for review and signature.
3. The signed original will be saved and maintained electronically.

C. Record of Business Associate Agreement

The Privacy Officer/designee will maintain a listing of all Business Associate Agreements. This list shall include all Business Associate Agreements written or received by Arc GLOW. On an annual basis, Program Directors/Vice Presidents will review the list of active contractors and consultants with the Vice President of Compliance and Privacy Officer to ensure all necessary signed agreements are on file for entities meeting the definition of a Business Associate.

VIOLATIONS REMINDER

As stated above, the agency's Privacy Officer has general responsibility for implementation of this HIPAA Privacy Plan. Members of our agency workforce (as defined above) who violate this policy will be subject to disciplinary action up to and including termination of employment or contract with Arc GLOW. Anyone who knows or has reason to believe that another person has violated a policy should report the matter promptly to his/her Supervisor, Program Director/Vice President, or the agency's Privacy Officer.

All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, Arc GLOW will make every effort to handle the reported matter confidentially.

Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with Arc GLOW.

QUESTIONS

If you have questions about compliance with this HIPAA Privacy Plan, please contact your Department Director/Vice President or the agency's Privacy Officer immediately. It is important that all questions be resolved as soon as possible to ensure protected health information is used and disclosed appropriately.