HIPAA PRIVACY AND SECURITY POLICIES AND PROCEDURES OF
Cancer Center Oncology Medical Group, Inc.

Implementation and effective [*Insert effective date*]

Policy author(s):_____, Privacy Official
_____, Security Official

Reviewed by: _____,
Date: _____

Approved by: _____,
Date: _____

[*Insert name of Health Care Provider*]
[*Insert address*]
[*Insert phone number*]

TABLE OF CONTENTS

		Page
1.	**GENERAL INFORMATION APPLICABLE TO ALL PRIVACY AND SECURITY POLICIES**	**5**
	1.1 POLICY STATEMENT	5
	1.2 SCOPE OF THESE PRIVACY AND SECURITY POLICIES	5
	1.3 APPLICABILITY OF THESE POLICIES	5
	1.4 DEFINED TERMS	5
	1.5 DEFINITIONS	6
2.	**COMPLIANCE AND OVERSIGHT RESPONSIBILITIES OF THE PRIVACY OFFICIAL AND SECURITY OFFICIAL**	**11**
	2.1 PURPOSE OF POLICY	11
	2.2 POLICY DETAIL	11
	2.3 RESPONSIBILITIES OF THE PRIVACY AND SECURITY OFFICIAL	11
3.	**NOTIFICATION OF PRIVACY OR SECURITY BREACHES**	**12**
	3.1 PURPOSE OF POLICY	12
	3.2 POLICY DETAIL	12
4.	**NOTICE OF PRIVACY PRACTICES PROCEDURES**	**16**
	4.1 PURPOSE OF POLICY	16
	4.2 POLICY DETAIL	16
	4.3 WHO IS AFFECTED	17
5.	**MINIMUM NECESSARY STANDARD**	**18**
	5.1 PURPOSE OF POLICY	18
	5.2 APPLICABILITY	18
	5.3 POLICY DETAIL	18
	5.3.2 SENSITIVE INFORMATION.	20
6.	**INDIVIDUAL'S REQUEST TO RESTRICT USES AND DISCLOSURES OF PHI**	**22**
	6.1 PURPOSE OF POLICY	22
	6.2 POLICY DETAIL	22
7.	**INDIVIDUAL'S REQUEST FOR CONFIDENTIAL COMMUNICATIONS**	**24**
	7.1 PURPOSE OF POLICY	24
	7.2 POLICY DETAIL	24
8.	**INDIVIDUAL'S RIGHT OF ACCESS TO PHI**	**25**
	8.1 PURPOSE OF POLICY	25
	8.2 POLICY DETAIL	25
9.	**INDIVIDUAL'S REQUEST TO AMEND PHI**	**29**
	9.1 PURPOSE OF POLICY	29
	9.2 POLICY DETAIL	29
10.	**INDIVIDUAL'S REQUEST FOR AN ACCOUNTING OF DISCLOSURES**	**32**
	10.1 PURPOSE OF POLICY	32
	10.2 POLICY DETAIL	32

11. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS 35
11.1 PURPOSE OF POLICY 35
11.2 POLICY DETAIL 35
12. WAIVER OF RIGHTS 36
12.1 PURPOSE OF POLICY 36
12.2 POLICY DETAIL 36
13. DOCUMENTATION REQUIREMENTS AND RETENTION OF RECORDS 37
13.1 PURPOSE OF POLICY 37
13.2 POLICY DETAIL 37
14. AUTHORIZATIONS 39
14.1 PURPOSE OF POLICY 39
14.2 POLICY DETAILS 39
15. PERMITTED DISCLOSURES OF PHI 40
15.1 PURPOSE OF POLICY 40
15.2 POLICY DETAILS 40
16. DISCLOSURES TO BUSINESS ASSOCIATES 47
16.1 PURPOSE OF POLICY 47
16.2 POLICY DETAILS 47
17. DE-IDENTIFIED INFORMATION AND LIMITED DATA SETS 48
17.1 PURPOSE OF POLICY 48
17.2 POLICY DETAILS 48
18. COMPLAINTS 50
18.1 PURPOSE OF POLICY 50
18.2 POLICY OF DETAILS 50
19. DESIGNATED RECORD SETS 51
19.1 PURPOSE OF POLICY 51
19.2 POLICY DETAILS 51
20. DESIGNATED PERSONNEL/ACCESS PROFILES 52
20.1 PURPOSE OF POLICY 52
20.2 POLICY DETAIL 52
21. STATE LAW COMPLIANCE 53
21.1 PURPOSE OF POLICY 53
21.2 POLICY DETAIL 53
21.3 PROCEDURAL GUIDANCE 53
22. USE AND DISCLOSURE OF PSYCHOTHERAPY NOTES 54
22.1 BACKGROUND 54
22.2 POLICY 54
24. FUNDRAISING 55
24.1 PURPOSE OF POLICY 55
24.2 POLICY DETAIL 55
25. SALE OF PROTECTED HEALTH INFORMATION 56
25.1 PURPOSE OF POLICY 56
25.2 POLICY DETAIL 56
26. SOCIAL MEDIA POLICY 57

26.1 PURPOSE 57
26.2 SCOPE OF POLICY 57
26.3 WORK RELATED SOCIAL MEDIA USE AND SHARING 57
26.4 PERSONAL SOCIAL MEDIA USE 57
26.5 CONFIDENTIAL INFORMATION 58
26.6 PROTECTED HEALTH INFORMATION 58
26.7 OTHER PROHIBITED ACTIVITY 59
26.8 VIOLATIONS 59
PART 2 POLICY **60**
27. TRAINING ON HIPAA PRIVACY AND SECURITY POLICIES **71**
27.1 POLICY STATEMENT 71
27.2 SCOPE OF THIS POLICY 71
27.3 PURPOSE OF POLICY 71
27.4 POLICY DETAIL 71
28. DISCIPLINARY SANCTIONS FOR NONCOMPLIANCE WITH PROVIDER'S PRIVACY AND SECURITY POLICIES **73**
28.1 PURPOSE OF POLICY 73
28.2 POLICY DETAIL 73
29. REPORTING AND MITIGATING INADVERTENT OR IMPROPER DISCLOSURES OF PHI OR SECURITY INCIDENTS **74**
29.1 PURPOSE OF POLICY 74
29.2 POLICY DETAIL 74
30. ADMINISTRATIVE, TECHNICAL AND PHYSICAL PRIVACY AND SECURITY SAFEGUARDS **76**
30.1 PURPOSE OF POLICY 76
30.2 POLICY DETAIL 76
31. VERIFICATION OF PERSONS REQUESTING PHI **84**
31.1 PURPOSE OF POLICY 84
31.2 POLICY DETAILS 84

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

1. GENERAL INFORMATION APPLICABLE TO ALL PRIVACY AND SECURITY POLICIES

1.1 POLICY STATEMENT

It is the policy of Cancer Center Oncology Medical Group, Inc. (**Provider**) to Use and Disclose Protected Health Information (**PHI**) only for the purpose of Provider's Treatment, Payment, or Health Care Operations purposes or as otherwise allowed by law.

Provider will comply with applicable state laws except to the extent that it is not possible to comply with state law and the federal Health Insurance Portability and Accountability Act (**HIPAA).** Provider will consult with legal counsel when questions arise regarding the applicability of state law.

These policies are designed to comply with HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009 (**HITECH Act**).

These policies and procedures are not a contract and do not create and are not intended to create any third party rights (including, but not limited to, rights of patients, patient family members, or business associates). Provider reserves the right to change or amend these policies at any time (including retroactively) without notice. To the extent these policies and procedures establish requirements and obligations above and beyond those required by HIPAA, these policies and procedures are aspirational and shall not be binding on Provider.

1.2 SCOPE OF THESE PRIVACY AND SECURITY POLICIES

These policies apply to the Provider with respect to the PHI of individuals obtained in the course of administering and providing health care items or services.

1.3 APPLICABILITY OF THESE POLICIES

These policies are intended to guide the Provider’s Workforce Members about how they are to protect the PHI of individuals in carrying out their functions.

1.4 DEFINED TERMS

Certain words in these policies are defined terms and have a specific meaning. The defined terms and their definitions are generally set forth below, and may be more specifically addressed in the Privacy Rule and Security Rule.

1.5 DEFINITIONS

"**Affiliated Covered Entity**" means a single HIPAA covered entity comprised of legally separate covered entities that are under common ownership or control, as defined at 45 C.F.R. § 164.105(b)(1).
"**Breach**" is the acquisition, access, Use or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.
"**Business Associate**" is a person or entity who has been retained to carry out various functions on behalf of Provider which require that it receive PHI from Provider, or create and/or maintain PHI on behalf of Provider. Business Associates are required to sign a contract that obligates them to protect individuals' PHI in the same way as does Provider.
"Covered Entity" means a health care provider who transmits any health information in electronic form in connection with a transaction subject to HIPAA electronic standards; a health plan, or a health care clearinghouse.
"**Designated Record Set**" means a group of records maintained by or for Provider that are medical and billing records about individuals; enrollment, payment, claims adjudication records; or records Used, in whole or in part, by or on behalf of Provider to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, Used, or disseminated by or for Provider in written or electronic format. See also policy "XXIV. Designated Record Set."
"**Disclosure**" means the release, transfer, provision of access to, or divulging in any other manner information outside the entity holding the information.
"ePHI" means PHI stored or maintained electronically.
"**Health Care Operations**" generally include: (i) quality assessment activities; (ii) reviewing the qualifications of health care professionals; (iii) underwriting, premium writing and other activities relating to creating, obtaining, or renewing health insurance or health benefits, including a contract of reinsurance or stop-loss insurance obtained in connection with the provision of health plan benefits, either directly or indirectly; (iv) conducting or arranging for medical review, legal services, and auditing functions including fraud and abuse detection and any required compliance programs; (v) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating Provider; (vi) creating de-identified information or limited data sets, if needed; and (vii) business management and general administrative activities of Provider.
"**Health Oversight Agency**" means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
"**Health Oversight Activities**" means oversight activities of a health oversight agency authorized by law including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions or other actions necessary for appropriate oversight of the health care system, government benefit programs for which health information is relevant to beneficiary eligibility, entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards, or entities subject to civil rights laws for which health information is necessary for determining compliance. Health oversight activities do ***not*** include requests for an investigation or other activity in which the individual is the subject of the investigation or activity and *such investigation or other activity does not arise out of and is not directly*

related to: (i) The receipt of health care; (ii) A claim for public benefits related to health; or (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

"**HHS**" means the United States Department of Health and Human Services.

"**HIPAA**" means the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, codified at 42 U.S.C. §1320d through d-9, as amended.

"**HIPAA Policy Manual**" means all of the policies and procedures provided in this *HIPAA* manual,

"**HIPAA Rules**" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

"**Hybrid Entity**" means a single legal entity that is a covered entity; whose business activities include both covered and non-covered functions; and that designates health care components of the Covered Entity. For example, a health care provider that has a research laboratory may choose to designate itself as a hybrid entity and exclude the laboratory from its health care component. A component must be included in the covered portion of the Hybrid Entity if it would meet the definition of a Covered Entity or Business Associate if it were a separate legal entity. Health care components also may include a component only to the extent it performs covered functions.

"**Individual**" means the Patient or other person who is the subject of the protected health information. The term also includes personal representatives who are entitled to act on behalf of an Individual as provided in the HIPAA Privacy Rule. Such personal representatives may include (i) a parent of the Individual if the Individual is a minor; (ii) a person empowered under the Individual's Power of Attorney; (iii) a legal guardian, whether the individual is an adult or minor; or (iv) an executor/administrator of the Individual's estate.

"**Law Enforcement Official**" means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, or to prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

"**Limited Data Set**" is Protected Health Information that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

- Names.
- Postal address information, other than town or city, state and zip code.
- Telephone numbers.
- Fax numbers.
- Electronic 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.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.

"**Notice of Privacy Practices**" is a document that must be maintained by most Covered Entities that explains to individuals how the Covered Entity may Use and Disclose their PHI.

"**Organized Health Care Arrangement**" has the definition set forth in 45 C.F.R. §160.103 and includes, among other things, a clinically integrated care setting, such as a hospital, in which individuals typically receive health care from more than one health care provider.
"**Patient**" means the Individual.
"**Part 2 Policy**" means the addendum to this Policy that applies to Provider's Part 2 Programs rendering Substance Use Disorder treatment services to patients. In the event of any conflict between this *HIPAA Policy Manual* and the *Part 2 Policy*, the *Part 2 Policy* shall govern with respect to Part 2 Programs.
"**Part 2 Program**" means a Federally Assisted Program as defined in the *Part 2 Policy*.
"**Patient**" means the Individual.
"**Payment**" includes a broad range of activities undertaken by Provider to obtain reimbursement for the provision of health care, including:

- determinations of eligibility or coverage;
- adjudication or subrogation of health benefit claims;
- billing, claims management and collection activities;
- obtaining payment under a contract of reinsurance, including stop-loss or excess loss insurance,;
- review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care and justification of charges;
- utilization review activities, including pre-certification and pre-authorization, concurrent and retrospective review;
- Disclosure to consumer reporting agencies of only the following Individual information that is related to the collection of reimbursements:
  - Name and address.
  - Date of birth.
  - Social Security number.
  - Payment history.
  - Account number (if any).
  - The name and address of the Individual's health care provider and/or his or her health plan.

"**Privacy Official**" means the Individual with the authority to make or amend policies and procedures, delegate functions, execute Business Associate Agreements, and to perform other duties necessary to comply with the Privacy Rule. The term "Privacy Official" shall refer to the Privacy Official's designee when the Privacy Official has delegated a particular task or function to the designee.
"**Privacy Rule**" means the Standards for Privacy of individually Identifiable Health Information, as published in 45 C.F.R. Parts 160 and 164.
"**Program**" shall have the meaning defined in the *Part 2 Policy* to this Policy.
"**Protected Health Information**" or "**PHI**" means any information, whether oral or recorded, in any form or medium that is created by a health plan, a health care provider, a health care clearinghouse, or an employer that relates to the past, present or future physical or mental health of an Individual, including the provision of and payment for health care, that either identifies the Individual or provides a reasonable basis for such identification, except for health information in certain educational records. PHI does not include de-identified health information. PHI specifically includes protected health information stored or maintained electronically ("ePHI"). PHI does not include employment records held by a Covered Entity in its role as employer, or information regarding a person who has been deceased for more than 50 years. In the context of Part 2, PHI includes patient identifying information, including but not limited to the name, address, social security number, fingerprints, photograph, and similar information by which the identity of a patient can be determined with reasonable accuracy either directly or by reference to other information.
"**Provider**" means Cancer Center Oncology Medical Group, Inc.

"Required by Law" means a mandate contained in law that compels an entity to make a Use or Disclosure of protected health information and that is enforceable in a court of law.

"**Secretary**" means the Secretary of the United States Department of Health and Human Services.

"**Security Incident**" means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

"Security Official" means the Individual with the authority to make or amend policies and procedures, delegate functions, and perform other duties necessary to comply with the Security Rule. The term "Security Official" shall refer to the Security Official's designee when the Security Official has delegated a particular task or function to the designee.

"Security Rule" means the Health Insurance Reform: Security Standards, as published in 45 C.F.R. Parts 160 and 164.

"**Standard Transactions**" means the electronic transmission of information between two parties to carry out financial or administrative activities related to health care in the standardized format (including code sets and data elements) set forth under the HIPAA Standards for Electronic Health Care Transactions.
"**Substance Use Disorder**" or "**SUD**" shall have the meaning defined in the *Part 2 Policy* to this Policy.
"Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
"**Unsecured Record**" means any Record that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the Use of a technology or methodology specified by the Secretary in the guidance issued under Public Law 111-5, section 13402(h)(2).
"**Use**" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an entity maintaining such information.
"**Workforce**" or "**Workforce Member**" means and includes current employees, and other persons whose conduct, in the performance of work at the Provider are under the direct control of the Provider, whether or not they are paid by the Provider. Provider's workforce includes those Provider employees who are responsible for the administration of Provider and listed under the *Minimum Necessary Standard Policy*.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

2. COMPLIANCE AND OVERSIGHT RESPONSIBILITIES OF THE PRIVACY OFFICIAL AND SECURITY OFFICIAL

2.1 PURPOSE OF POLICY

To describe the roles of the Privacy Official and Security Official.

2.2 POLICY DETAIL

Provider has designated [Insert Individual title(s)] Privacy Official and Security Official to coordinate and oversee implementation of these policies and procedures. The Privacy Official and Security Official are responsible for monitoring the Provider's compliance with these policies, its contracts, and its BA Agreements. The Privacy and Security Officials may consult with legal counsel prior to recommending that the Provider enter into a particular BA agreement.

2.3 RESPONSIBILITIES OF THE PRIVACY AND SECURITY OFFICIAL

The Privacy and Security Officials are responsible for the development, implementation, maintenance and evaluation of the Provider's policies and procedures relating to PHI security and privacy. The Privacy and Security Officials' responsibilities include:

- Ensuring appropriate technical and non-technical risk analyses are performed at regular intervals, and in response to major structural or operational changes within the BA;
- Approving risk mitigation plans, risk prioritization and methods for the elimination or minimization of risks;
- Facilitating timely actions, decisions and remediation activities;
- Directing the development of, approving, and monitoring an appropriate training program;
- Directing the maintenance and revisions of the incident response policy and other required policies and procedures;
- Auditing and monitoring compliance with these policies and procedures;
- Providing guidance to the BA regarding interpretation and implementation of these policies and procedures;
- Ensuring that appropriate Subcontractor Agreements are signed;
- Responding to privacy and security complaints;
- Establishing mechanisms to comply with obligations to Covered Entities to track Disclosures of and access to PHI as required by law, and to make PHI available for access, amendment and accounting as required by the BA Agreements;
- Ensuring compliance with the policies and procedures by consistently imposing sanctions against Workforce Members for failing to comply, in cooperation with the BA's human resources department;
- Maintaining knowledge of applicable federal and state privacy laws, and monitoring advancement in information privacy and security technologies;

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

- Cooperating with DHHS and other governmental oversight agencies in any compliance reviews and investigations.

DEPARTMENT:		POLICY TITLE:	
EFFECTIVE DATE:		APPROVAL DATE:	
APPROVED BY:		POLICY NO.:	
Regulations:			

3. NOTIFICATION OF PRIVACY OR SECURITY BREACHES

3.1 PURPOSE OF POLICY

To describe how Provider will comply with the HIPAA Rule and HITECH Act requirements regarding notifying individuals and required entities of Breaches.

3.2 POLICY DETAIL

To guard against and to detect potential Security Incidents and Breaches, Provider trains its workforce regarding proper Uses and Disclosures of PHI, and how to report suspected Security Incidents. Provider will provide written notification to affected individuals in those instances where Provider has determined based upon a risk assessment that there is more than a low probability that affected individuals' unsecured PHI has been compromised, thereby constituting a Breach under the HIPAA Rules and HITECH Act. A Breach is defined as the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

If a Security Incident, Breach, or suspect improper Use or Disclosure occurs, the Privacy Official, and if the PHI is electronic, the Security Official, must be notified immediately so they can initiate and coordinate an investigation. Law enforcement may need to be notified of a Breach or Security Incident, depending on the facts and circumstances. Law enforcement may request that a Breach notice be delayed. A law enforcement request for a delay in notification shall be documented. If the statement is in writing and specifies the time for which a delay is required, delay the notification for the time period specified by the official. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time. Notwithstanding the foregoing, if Provider is a Part 2 Program, the *Part 2 Policy* to this Policy applies to Disclosures to law enforcement and shall govern in the event of any conflict with the terms of this Policy.

There are certain exceptions to the notification requirement for individuals, but a notice to a Covered Entity or another Business Associate may still be required. An incident, including a Security Incident, will not be considered a Breach and notification to Individuals will not be required for:

1. Any unintentional acquisition, access, or Use of PHI by a Workforce Member or person acting under the authority of Provider, if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under the HIPAA Privacy Rule;
2. Any inadvertent Use or Disclosure by a person who is authorized to access PHI at Provider or a business associate to another person authorized to access PHI at the same Covered Entity or business associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under the Privacy Rule; or

3. A Disclosure of PHI where the Provider or business associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

A Breach is presumed unless the Provider or Business Associate demonstrates that there is a low probability that the unsecured PHI has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
b. The unauthorized person who Used the PHI or to whom the Disclosure was made;
c. Whether the PHI was actually acquired or viewed; and
d. The extent to which the risk to the PHI has been mitigated.

If ransomware is involved, the risk assessment should also consider the following additional factors:

e. Whether there is a high risk of unavailability of PHI; and
f. Whether there is a high risk to the integrity of the PHI.

Breaches of unsecured PHI require notification to the individuals whose information was subject to the Breach, as well as to the Department of Health and Human Services, and possibly to the media. The HIPAA Rules define "unsecured protected health information" as PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the Use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5." If the PHI involved in the incident was encrypted in accordance with industry standards, and the decryption key was maintained in a secure manner, it is unlikely that the PHI would be considered “unsecured protected health information” and, therefore, a reportable Breach is unlikely.

Within 60 days of a Breach of unsecured PHI, or within a shorter time that may be required by state law, notices should be sent to the affected Individuals via first class mail when address information is available. If the person has expressed a preference to accept communications electronically, an e-mail notification is allowed.

If the Breach involves PHI of more than 500 people in one state or jurisdiction, a notice must be provided to prominent media outlets serving that state or jurisdiction.

If the Breach involves PHI of 10 or more individuals for whom there is no current address, a web site notice must be posted as a substitute notice, or a notice must be placed in major print or broadcast media, including major media in geographic areas where the individuals affected by the Breach likely reside. In the case where there is insufficient contact information for fewer than 10 individuals, substitute notice may be provided by other written notice, telephone or through other means.

If urgent notice is required because of possible imminent misuse of unsecured PHI, notice may be provided by telephone in addition to other notices required under this policy. If a Breach involves Social Security numbers, bank account numbers, or similar information, there may be applicable state laws which must also be followed.
If the Breach involves unsecured PHI of 500 or more individuals, notice must be provided to the federal Department of Health and Human Services (HHS) immediately. This should be done online through the HHS Office for Civil Rights web portal. If fewer than 500 individuals are involved, the Breach must be maintained in

a log and reported to HHS no later than 60 days after the close of the calendar year in which the Breach was discovered.

Notices governed under both state law and HIPAA must comply with both sets of laws, unless it is impossible to comply with both, in which case the more stringent law governs. Documentation related to the Breach and subsequent notice must be maintained for six years or longer as required by applicable law.

When notification is required, Provider should advise the affected individuals utilizing the Provider's adopted notice form. If no notice form has been adopted, then notice should be provided similar to the following, depending on the facts and state law requirements:

[*Company letterhead*]

[*Date*]

VIA FIRST CLASS MAIL [*Note: May be sent via e-mail if Individual has indicated a preference for that and has agreed to it in writing*.]

[*Last known address of Individual*]

Dear:

On behalf of Cancer Center Oncology Medical Group, Inc. ("Company"), I am writing to you because a recent incident may have involved your protected health information. We have learned that there is a possibility that an unauthorized person accessed a _____ containing medical records and other information. On _____, 20__, [*include a brief description of what happened, including the date of the Breach and the date of discovery, if known*]. We believe that the Individual(s) responsible may have had access to a database containing [*describe the types of unsecured protected health information that were involved in the Breach (e.g. full name, social security number, date of birth, etc.).*

[*Include a discussion of the steps individuals should take to protect themselves from potential harm resulting from the Breach, such as contacting credit bureaus and placing a fraud alert on the Individual's credit file.]*

[*Include a brief description of what the* Covered Entity *involved is doing to investigate the Breach, to mitigate loss, and to protect against any further Breaches. An example is below*.]

Provider has filed a law enforcement report with the [*insert agency*]. The incident report number is _____. Management immediately launched an internal investigation into this matter, and began taking steps to reduce the risk of future unauthorized access to information. Once we have compiled all relevant facts, we will consider additional action as necessary to prevent the theft of personally identifiable information. While we are uncertain whether your personal information was actually obtained during the unauthorized access, we want to bring this situation to your attention, and urge you to take actions to minimize your potential risk of identity theft.

We want to assure you that we take our responsibility to safeguard personal information very seriously. As a result of this incident, we are also undertaking further steps to increase this security, such as _____.

If there is anything Company can do to assist you, of if you have any questions or require additional information, please contact us at _____ [*must include a toll-free telephone number, an e-mail address, Web site, or postal address*].

We apologize for any inconvenience or concern this incident may cause you. [*Note whether additional information will be provided in a later mailing*.]

Sincerely,

_____

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

4. NOTICE OF PRIVACY PRACTICES PROCEDURES

4.1 PURPOSE OF POLICY

This policy outlines how Provider will provide the Notice of Privacy Practices ("Notice") to patients. Provider will provide each patient with adequate notice of the Uses and Disclosures of PHI that may be made by the Provider, and of the patient's right and the Provider's legal duties with respect to PHI. Provider shall update the Notice from time to time.

4.2 POLICY DETAIL

The Provider and Workforce Members will follow the steps set forth below to provide each patient with adequate notice of the Uses and Disclosures of PHI that may be made by the Provider, and of the patient's rights and the Provider's legal duties with respect to PHI.

- **STEP 1: PROVISION OF NOTICE**. Except in an emergency, the Provider will provide a copy of the Notice of Privacy Practices to patients no later than the date of the first service delivery (including service delivered electronically) and to any member of the public who requests one. In emergency treatment situations, the Provider shall provide a copy of the Notice to patients as soon as reasonably practicable after the emergency treatment.

- **STEP 2: ACKNOWLEDGMENT OF RECEIPT.** Except in an emergency, the Provider will make a good faith effort to obtain a written acknowledgment of receipt of the Notice. If a Provider is unable to obtain the acknowledgement, the Provider shall document its attempt to obtain the acknowledgement and the reason for not obtaining it.

- **STEP 3: AVAILABILITY ON REQUEST.** The Provider will make the Notice available upon request.

- **STEP 4: POSTING OF NOTICE.** In addition to providing a copy of the Notice in accordance with Step 1, the Provider will post a copy of the Notice in a clear and prominent location where it is reasonable to expect the Provider's patients to be able to read the Notice.

- **STEP 5: WEBSITE.** The Provider will prominently post the Notice on the entity's web site and make the Notice available electronically through that web site. If the first service delivery to a patient is delivered electronically, the Provider will provide electronic Notice automatically and contemporaneously in response to the patient's first request for service. The Provider will maintain a record of the Individual's acknowledgment that they received the electronic Notice. The patient who is the recipient of electronic Notice retains the right to obtain a paper copy of the Notice upon request.

- **STEP 6: REVISIONS TO NOTICE.** The Provider will revise the Notice, and implement the revised Notice, within 60 days of a material change to the Uses or Disclosures, the patient's rights, the

Provider's Legal duties, or other privacy practices stated in the Notice. Whenever the Notice is revised, the Provider will make the Notice available upon request on or after the effective date of the revision.

- **STEP 7: DOCUMENTATION.** The Provider will retain a representative copy of each Notice it distributes for 6 years from the date when it last was in effect.

  The Provider will retain the written acknowledgments (or documentation of good faith efforts to obtain written acknowledgment) for 6 years.

4.3 WHO IS AFFECTED

Provider and Workforce Members must follow this Policy.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

5. MINIMUM NECESSARY STANDARD

5.1 PURPOSE OF POLICY

To ensure compliance with the HIPAA Privacy Rule regarding the minimum necessary requirements for requests for the Uses or Disclosures of PHI.

5.2 APPLICABILITY

Provider and Workforce Members must follow this Policy. However, if Provider is a Part 2 Program providing Substance Use Disorder treatment, the *added Policy* to this *HIPAA Policy Manual* applies and shall govern in the event of any conflict with the terms of this Policy.

5.3 POLICY DETAIL

Provider will:

- identify those persons or classes of persons in its Workforce who need access to PHI to carry out their duties with respect to treatment, payment, or health care operations;
- determine the access needed and any conditions appropriate to such access by those persons or classes of persons; and
- make reasonable efforts to limit the access of such persons or classes to PHI consistent with this Policy.

Provider's Workforce Use of Relevant Records Offsite. Provider employees are restricted from keeping, accessing and transporting records containing PHI outside of the Provider's premises, except as expressly permitted herein.

Monitoring of the Policies and Procedures Governing Access to PHI. The Security Official and/or Privacy Official will regularly monitor the Provider's policies and procedures designed to protect PHI to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to, or Use of PHI. The Security Official and/or Privacy Official will identify appropriate revisions or upgrades to the Provider's policies and procedures to reduce and mitigate the risk of unauthorized access to or Use of PHI.

Access to Relevant Records. The Security Official and/or Privacy Official is responsible for the management of exiting employees including, but not limited to, terminated employees, retiring employees, and employees who have voluntarily resigned from their employment at the Provider (collectively, the "Exiting Employees") The Security Official and/or Privacy Official will take steps to ensure that Exiting Employees are prevented from having access to records containing PHI prior to their leaving the premises after being terminated. Access removal includes both physical and electronic access. Steps taken to ensure that access is removed include, at a minimum: (i) deactivating applicable User accounts and passwords, (ii) confiscating keys to file cabinets and other storage areas containing PHI in the Exiting Employee's control, (iii) confiscating keys or ID badges that would allow the Exiting Employee to access Provider physical premises, and (iv) notifying building security that a particular Exiting Employee has been terminated.

Return of Relevant Records. The Security Official and/or Privacy Official will collect from the Exiting Employee (i) all records containing PHI, in any form or medium, currently in the Exiting Employee's possession or control, and (ii) all copies of records containing PHI, in any form or medium, currently in the Exiting Employee's possession or control.

Provider's Workforce Obligations. In addition to the other responsibilities set out in these policies, each Provider Workforce Member shall be responsible for:

- Regularly reviewing these policies, including all revisions and updates that are made to these policies and procedures to the extent they are relevant to the Workforce Member's job duties;
- Complying with all relevant policies and procedures that have been developed and implemented;
- Executing such Workforce Member's confidentiality agreement (if applicable), and returning an executed copy to the Security Official and/or Privacy Official;
- Understanding and complying with any responsibilities given to such employee pursuant to these policies, including all related development, implementation, monitoring and maintenance obligations;
- Knowing and complying with all policies and procedures related to the access, Use and treatment of all records containing PHI;
- To the extent they are relevant to the Workforce Member's job duties, reviewing all internal and external risks identified in audits in accordance with these policies in order to be more aware of potential threats to the integrity and security of records containing PHI;
- Providing feedback and suggestions to the Security Official and /or Privacy Official relating to the policies and procedures implemented to protect PHI;
- Reporting to the Security Official and/or Privacy Official all suspicious activity relating to records containing PHI such as unauthorized Use of such records by other employees, or unauthorized attempts to access such records by other parties;
- Immediately reporting any discovered Security Incidents or Breaches to the Security Official and or Privacy Official;
- Understanding and complying with all physical and electronic security measures adopted to protect the integrity and confidentiality of PHI;
- Refraining from using, storing or transmitting PHI in an unauthorized manner including, but not limited to, "snooping," viewing records without a legitimate business need, or transmitting PHI in an unsecure manner (e.g., emailing PHI without encryption);
- Refraining from storing any PHI on employee personal devices, such as cell phones or tablets;

- Refraining from sharing PHI on social media or in other unauthorized avenues;
- Protecting all assigned passwords so that they are not accessible or Used by other parties; and
- Complying with all exit requirements when the Workforce Member leaves employment (including returning keys, and any PHI or other confidential materials in the Workforce Member's possession).

ROUTINE/RECURRING DISCLOSURES. Any type of Disclosure that Provider makes on a routine and/or a recurring basis will be made in accordance with standard protocols developed by Provider with respect to each type of routine or recurring Disclosure so as to limit the PHI Disclosed to the amount reasonably necessary to achieve the purpose of the Disclosure.

6.3.2 SENSITIVE INFORMATION.

To the extent that Provider receives a request to Disclose or otherwise Use sensitive information, including psychotherapy notes or SUD counseling notes, such request should be relayed to Privacy Officer, as appropriate to ensure such Use and Disclosure is proper/secure. Sensitive information is information that is more likely to result in harm, embarrassment, or unfairness to an Patient. Examples of sensitive information may include information related to HIV/AIDS information, substance abuse treatment information, and mental health information. Additional precautions should be taken with sensitive information.

DISCLOSURES: MINIMUM NECESSARY STANDARD APPLIES. For all other Disclosures to which the Minimum Necessary Standard applies, Provider will:

- utilize a Limited Data Set whenever practicable;
- utilize criteria designed to limit the PHI Disclosed to the information reasonably necessary to accomplish the purpose for which Disclosure is sought; and
- review requests for Disclosure on an Individual basis in accordance with such criteria.

Provider may rely, if such reliance is reasonable under the circumstances, on a requested Disclosure as the minimum necessary for the stated purpose when:

- making Disclosures to public officials that are permitted under the HIPAA Privacy Rule, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
- the information is requested by another Covered Entity;
- the information is requested by a professional who is a member of Provider's workforce or is a Business Associate of Provider for the purpose of providing professional services to Provider, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
- a person who is requesting the information for research purposes and who has provided documentation or representations that comply with the applicable Privacy Rule.

Provider will limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other Covered Entities. Provider may not Use, Disclose or request an entire medical record, except when the entire record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the Use, Disclosure, or request.

6.3.4 DISCLOSURES: MINIMUM NECESSARY STANDARD DOES NOT APPLY.

The Minimum Necessary Standard does ***not*** apply to the following kinds of Disclosures or requests:

- Disclosures to or requests by a health care provider for Treatment.
- Disclosures to the Individual whose PHI is being Disclosed pursuant to their request.
- Disclosures made pursuant to a HIPAA-compliant authorization.

- Disclosures made to the Secretary.
- Disclosures that are Required by Law.
- Disclosures that are necessary to comply with applicable requirements of the Privacy Rule.

PROVIDER'S WORKFORCE. Access privileges for Individual Workforce Members will be terminated or changed in conjunction with the termination of employment, contract, or change of level of access required. Provider's IT servicers will audit the access privileges on a regular basis and shall report to Security Official and/or Privacy Official if any changes are needed.

Job Class	Categories of PHI to Which Workforce Member Needs Access	Access Profile (Physical and electronic)
Privacy Official Security Official		Unlimited Access: Unlimited access to PHI, including demographic information, medical information, and enrollment data, is necessary for the operation of Provider and verification of compliance with HIPAA. Complete access to Individual files, copy machines, fax machines, data screens.
Legal Counsel		Limited Access: Limited access required as needed to provide legal advice to Provider. The Privacy Official will determine necessary access on a case-by-case basis.
IT Group		
Risk Manager		
[*Insert other workforce members*]		

Access to Provider's systems shall be immediately terminated upon the resignation or termination of any workforce member.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

7. INDIVIDUAL'S REQUEST TO RESTRICT USES AND DISCLOSURES OF PHI

7.1 PURPOSE OF POLICY

To ensure compliance with applicable laws regarding requests from individuals to restrict the Uses and Disclosures of their PHI.

7.2 POLICY DETAIL

Provider will permit an Individual to request restrictions on the Uses or Disclosures of the Individual's PHI to carry out Provider's Payment or Health Care Operations and other Uses and Disclosures that Provider is permitted to make under the HIPAA Privacy Rule. Any such request must be made in writing and sent to the Privacy Official. The Privacy Official may request that individuals make this request on Provider's template form for requesting restrictions.

DENIAL OF INDIVIDUAL'S REQUEST. While individuals are entitled to request that Provider restrict the Uses and Disclosures of the Individual's PHI that Provider would otherwise be permitted to make under the Privacy Rule, Provider is not required to agree to any particular restriction, with one exception set forth below. Provider will not agree to a request to restrict a Use or Disclosure that Provider is required to make under the Privacy Rule, or one that it is otherwise required by law to make.

APPROVAL OF INDIVIDUAL'S REQUEST. If Provider agrees to a particular restriction, Provider may not Use or Disclose PHI contrary to such restriction and Provider will document the restriction. Provider shall agree to an Individual's request to restrict the Disclosure of PHI to a health plan if:

- The Disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

- The PHI pertains solely to a health care item or service for which the Individual, or person other than the health plan on behalf of the Individual, has paid the Covered Entity out-of-pocket in full. Provider, however, may Use the restricted PHI, or may Disclose such information to another health care provider to provide emergency treatment to the Individual if the Individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment. Provider must request that such health care provider not further Use or Disclose the information.

TERMINATING THE RESTRICTION. Provider may terminate the restriction if:

- The Individual requests and agrees in writing that the restriction be terminated;
- The Individual orally requests and agrees that the restriction be terminated and the oral request and agreement is documented; or

- Provider informs the Individual that it is terminating its agreement to restrict Provider's Use or Disclosure of the Individual's PHI, except that such termination is only effective with respect to PHI created or received after Provider has so informed the Individual.

If Provider decides to rescind a previously agreed to restriction, it will so inform the Individual and document its termination of the restriction.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

8. INDIVIDUAL'S REQUEST FOR CONFIDENTIAL COMMUNICATIONS

8.1 PURPOSE OF POLICY

To ensure compliance with the Privacy Rule regarding confidential communications.

8.2 POLICY DETAIL

Individuals may request that Provider communicate with them in a more confidential fashion than Provider's standard communication procedures otherwise provide. Individuals must make these requests in writing to the Privacy Official. The Privacy Official may ask individuals to Use Provider's form for these requests. Provider intends to comply with reasonable confidentiality requests and will not require that the Individual explain the basis or reasons for the request.

Provider will try to provide reasonable accommodation for a confidentiality request by:

- limiting or modifying the information provided with respect to requests for Payment;
- sending information to the Individual at an alternative address or other method of contact.
- sending information to the Individual in a manner that conceals the information from anyone but the addressee (*e.g.*, sending information in sealed envelopes); and
- not providing identification on the outer envelope that the content contains medical information or is from Provider.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

9. INDIVIDUAL'S RIGHT OF ACCESS TO PHI

9.1 PURPOSE OF POLICY

To identify how Provider will process a request from an Individual to inspect and/or obtain a copy of their own PHI that is maintained in Provider's Designated Record Set.

9.2 POLICY DETAIL

Provider will permit an Individual to request access to inspect or to obtain a copy of the Individual's own PHI that is maintained in Provider's Designated Record Set. Individuals who wish to inspect their PHI, rather than receive a copy, will be accommodated.

Individuals may make requests for access in writing on the forms adopted by Provider or the Individual may require the Provider to transmit a copy of PHI directly to another person designated by the Individual. The Individual's request to send PHI to a third party must be in writing, signed by the Individual, and clearly identify the designated person and where to send the copy of the PHI.

NO RIGHT TO ACCESS. An Individual's right of access does not include:

- psychotherapy notes;
- SUD counseling notes or
- information compiled in reasonable anticipation of, or for Use in, a civil, criminal, or administrative action or proceeding.

DENIAL OF ACCESS. Provider may deny an Individual access ***without*** providing the Individual an opportunity for review, in any of the following circumstances:

- The PHI is exempt from the right of access, as noted above.
- Provider, when acting under the direction of a correctional institution, may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such information would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
- An Individual's access may be denied if the PHI was obtained from someone other than Provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Access may be denied to an Individual, but the Individual has the right to have the denials reviewed, in the following circumstances:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Individual or another person. Denial of access under this section is not permitted if the concern merely relates to emotional harm only.

- The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
- The request for access is made by the Individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the Individual or another person.

If access is denied as outlined above, the Individual has the right to have the denial reviewed by a licensed health care professional who is designated by Provider to act as a reviewing official and who did not participate in the original decision to deny. Provider will provide or deny access in accordance with the determination of the reviewing official. Provider must promptly provide written notice to the Individual of the reviewing official's determination.

If access to PHI is ***denied***, in whole or in part, Provider:
- must, to the extent possible, give the Individual access to any PHI requested for which there is no basis for denying access; and
- must provide a timely, written denial to the Individual. The denial must be in plain language and contain the following:
  - The basis for the denial.
  - A statement that the Individual has the right to seek a review of the denial.
  - A statement that the Individual may file a complaint with Provider through Provider's Privacy Official, or with the Secretary.

If Provider determines that it does not maintain the PHI that the Individual wishes to see and Provider knows where the requested information is maintained, then Provider must inform the Individual where to direct the request.

TIME LIMITS. Provider will act on a reasonable request to inspect PHI no later than 5 business days after receipt of the request and provide copies within 15 days. All other requests shall be responded to as follows, a:

- If Provider ***grants*** the request, in whole or in part, Provider must inform the Individual of the acceptance of the request and provide the access requested.
- If Provider ***denies*** the request, in whole or in part, it must provide the Individual with a written denial.

If Provider is unable to take action on the request within the time limits provided, then Provider may seek to extend the time for such actions by no more than 15 days, provided that:
- Provider, within the applicable required time limit, provides the Individual with a written statement of the reasons for the delay and the date by which Provider will complete its action on the request; and
- Provider has only one such extension of time for action on a request for access.

Notwithstanding the foregoing, Provider will comply with any stricter time limits provided under applicable state law.

APPROVAL OF ACCESS. If access to PHI is granted by Provider to an Individual, then Provider must do the following:

- Provide the access requested by the Individual by allowing the Individual to inspect and/or copy his or her PHI that is maintained in Provider's Designated Record Set. If the PHI requested is maintained at more than one location, Provider need only produce the PHI once in response to a request.
- Provide the Individual with access to the PHI in a readable hard copy form, or in another form or format to which the Individual and Provider can agree. If the information is electronic, the Individual shall have a right to obtain from the Provider a copy of such information in an electronic format and, if the Individual chooses, to direct the Provider to transmit such copy directly to an entity or person designated by the Individual, provided that any such choice is clear, conspicuous, and specific.
- Provide the Individual with a summary of the PHI requested, in lieu of providing access to the PHI, or provide the Individual with an explanation of the PHI requested, if:
  (1) the Individual agrees in advance to such a summary or explanation; and
  (2) the Individual agrees in advance to the fees imposed, if any, by Provider for such summary or explanation.

Access will be provided as requested by the Individual in a timely manner, including arranging with the Individual a convenient time and place to inspect and/or obtain a copy of the PHI, or mailing any requested copy to the Individual.

REASONABLE FEES. Provider may impose a reasonable fee that aligns with state law for providing copies or summaries of PHI. Provider will notify the Individual in advance of the approximate fee, and will make available to individuals, upon request, an approximate fee schedule for regular types of access requests, which may include a breakdown of the charges for labor, supplies, and postage. The fee will only include: (1) the cost of copying, including the cost of supplies for and labor of copying; (2) postage, when the Individual has requested that the copy, or the summary or explanation, be mailed; and (3) expenses incurred in preparing an explanation or summary of the PHI, if the Individual agrees. The costs of providing PHI in electronic form shall not be greater than the Provider's labor costs in responding to the request for the copy (or summary or explanation).

Provider may calculate its labor costs through any of the following methods:

Actual costs: Provider may calculate the actual labor costs to fulfill the request, as long as the labor cost is only for copying (and/or creating a summary or explanation if the Individual chooses to receive a summary or explanation) and the labor rates Used are reasonable for such activity. Provider may add to the actual costs any applicable supply (e.g., paper, or CD or USB drive) or postage costs. Provider must be prepared to inform individuals in advance of the approximate fee that may be charged for providing the Individual with a copy of his or her PHI.

Average costs; Provider may develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are permissible (e.g. labor costs for copying but not for search and retrieval) and are reasonable. Provider may add to that amount any applicable supply (e.g., paper, or CD or USB drive) or postage costs. The standard rate may be calculated and charged as a per page fee only in cases where PHI requested is maintained in paper form and the Individual requests a paper copy of the PHI or asks that the paper PHI be scanned into an electronic format. Per page fees are not permitted for paper or electronic copies of PHI maintained electronically.

Flat fee: Provider may charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage.

If a higher fee is expressly permitted by state law or other law, Provider will not charge such fee in situations where the Individual is requesting access to his or her own record. Instead, Provider may charge a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI. Provider may charge a higher fee otherwise expressly permitted by other law if a third party is requesting the PHI on its own behalf through a HIPAA-compliant authorization form or some other lawful process.

Retaining Documentation. Provider must document the following and retain such documentation for a period of six years:

- Documentation of the components of Provider's Designated Record Set that individuals may access.
- The titles of the persons or offices responsible for receiving and processing requests for access.

INFORMATION BLOCKING REQUIREMENTS. A Patient request for records that are maintained electronically by Provider may also be required to meet the 21st Century Cures Act information blocking regulations. If records are available through the patient portal, such records must be made available in the portal at the same time such records are available to the physician unless an information blocking exception applies, the patient has requested that such records are not delivered to the portal or the patient requests the records in a different format. No fees may be imposed on the patient for electronic access to records. California law requires compliance with the federal information blocking law.

Request for Access to Protected Health Information

Patients or their personal representatives may inspect and/or obtain copies of certain protected health information maintained by or for [INSERT ENTITY NAME], in accordance with [INSERT ENTITY NAME] Policies and Procedures and federal regulations known as the HIPAA Privacy Rule. To assist us in responding to your request, please fill out the following information:

Patient's Name (Please print legibly): _____

Information Requested (Please check all that apply):

☐ All protected health information

☐ The following protected health information (please describe): _____

Type of Access Requested (Please check all that apply):

☐ I wish to inspect my protected health information.

☐ I wish to pick up a copy of the protected health information.

☐ I wish to have a copy of the protected health information mailed to the following person and location (specify name and address):

_____

Summary of Information: At your request, we will provide you with a summary of your protected health information to which you are granted access, instead of making that information available for inspection or providing a copy. If you request a summary by checking the box in this section, we will not arrange for your inspection or provide you with a copy of the information, even if you have checked one or more boxes in the preceding section.

☐ I wish to receive a summary instead of inspecting or receiving a copy of the information.

Fees: If you request a copy or summary of protected health information, we may charge a reasonable, cost-based fee for the preparation of the copy or summary. You will be informed of the fee in advance.

Form of Access Requested (e.g. paper copy, electronic copy): _____. We will provide you with access to the protected health information in the form or format you request if the protected health information is readily producible at a reasonable cost in such form or format. If not, we will provide you with a paper copy of the protected health information.

Person Requesting Access:

☐ Patient

☐ Personal representative (Print name legibly):_____

Please Sign:

Patient	Personal Representative
Date	Description of personal representative's authority to act for patient

We will provide you, or a third party you have designated, with a response to your request in a timely fashion in accordance with applicable law. We have the right in certain circumstances to deny access to all or part of the information you have requested.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

10. INDIVIDUAL'S REQUEST TO AMEND PHI

10.1 PURPOSE OF POLICY

To set forth the procedures whereby an Individual may file a request to amend his or her PHI maintained in Provider's Designated Record Set.

10.2 POLICY DETAIL

An Individual has the right to request that Provider amend his or her PHI that is in Provider's Designated Record Set for as long as Provider maintains that PHI in its Designated Record Set. Provider will require that individuals make their requests for amendment in writing to the Privacy Official. The Privacy Official may require individuals to make such requests on Provider's form for requesting amendments. In all cases, individuals must provide a reason to support the requested amendment.

DENIAL OF REQUEST. Provider is not obligated to grant the Individual's request. Provider may deny an Individual's request to amend Provider's Designated Record Set if it determines that the PHI or record:

- was not created by Provider, unless the Individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- is not part of Provider's Designated Record Set;
- would not be accessible by the Individual or available for inspection by the Individual under the Privacy Rule; or
- is accurate and complete.

Should Provider ***deny*** the requested amendment, in whole or in part, Provider must do the following:

- Provide the Individual with a timely, written denial. The denial must use plain language and contain the following:
  - The basis for the denial.
  - The Individual's right to submit a written statement disagreeing with the denial and how the Individual may file the "Statement of Disagreement."
  - If the Individual does not submit a Statement of Disagreement, the Individual may request that Provider provide the Individual's request for amendment and Provider's denial with any future Disclosures of the PHI that is the subject of the amendment.
  - A description of how the Individual may complain to Provider or to the Secretary pursuant to the procedures established in the HIPAA Privacy Rule. The description must include the name, or title, and telephone number of the contact person or office designated in the Privacy Rule.
- Permit the Individual to submit to Provider a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Provider may reasonably limit the length of a Statement of Disagreement to no more than a single page, single spaced, 12-point type for each denied amendment request.

- Elect or decline to prepare a written rebuttal to the Individual's Statement of Disagreement. Whenever such a "Rebuttal Statement" is prepared, Provider must provide a copy to the Individual who submitted the Statement of Disagreement.
- As appropriate, identify the record or PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the Individual's request for an amendment, Provider's denial of the request, the Individual's Statement of Disagreement, if any, and Provider's Rebuttal Statement, if any, to the Designated Record Set.
- If an Individual has submitted a written Statement of Disagreement, include the material appended in accordance with the paragraph above, or, at the election of Provider, an accurate summary of any such information, with any subsequent Disclosure of the PHI to which the disagreement relates.
- If the Individual ***has not*** submitted a written Statement of Disagreement, include the Individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure of the PHI only if the Individual has requested such action.

TIME LIMITS. Provider must either comply with or deny the Individual's request for an amendment no later than 60 days after receipt of the request. If Provider is unable to act on the amendment request within 60 days after the receipt of the request, Provider may seek to extend the time for its decision no more than 30 days if Provider, within the original 60-day time limit, provides the Individual with a written statement of the reasons for the delay and the date by which Provider will make its decision. Provider may have only one extension of time.

Notwithstanding the foregoing, Provider will comply with any stricter time limits for Designated Record Set amendments provided under applicable state law.

APPROVAL OF REQUEST. If Provider ***accepts*** the requested amendment, in whole or in part, Provider must:

- Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the revised information.
- Timely inform the Individual that the amendment has been accepted and obtain the Individual's help, if needed, to identify the relevant persons with which the amendment needs to be shared, and get the Individual's agreement for Provider to notify these persons.
- Make reasonable efforts to inform the following persons that certain records in the Designated Record Set have been amended and, within a reasonable period of time, to provide them with the amended information:
    - persons identified by the Individual as having received PHI about the Individual and needing the amendment; and
    - persons, including Business Associates, that Provider knows have in their records the PHI that is the subject of the amendment and who may have relied, or could reasonably rely, on such information to the detriment of the Individual.

When a subsequent Disclosure is made using a Standard Transaction under the Privacy Rule that does not permit the additional material to be included with the Disclosure, Provider may separately transmit the material required above, as applicable, to the recipient of the Standard Transaction.

In the event Provider is informed by another health care provider, health plan, or Business Associate of an amendment, Provider must amend the PHI in Provider's Designated Record Set that is the subject of that amendment.

The Privacy Official will be responsible for receiving and processing requests for amendments by individuals. Provider will retain the documentation as required by the Privacy Rule for a period of six years.

Request to Amend or Correct Protected Health Information

Patients or their personal representatives may submit a request in writing to have their protected health information amended or corrected in accordance with our Policies and Procedures and federal regulations known as the HIPAA Privacy Rule. The patient or personal representative must include a reason to support a requested amendment or correction. To assist us in responding to your request, please fill out the following information:

Amendment or Correction:

I. Name of Patient (please print legibly): _____

II. Please specifically describe the protected health information you would like amended or corrected (including dates): _____

_____

_____

_____

III. Please specifically describe how you would like the protected health information amended or corrected: _____

_____

_____

_____

IV. Please give specific reasons to support your requested amendment or correction: _____

_____

_____

_____

_____

Person requesting Amendment or Correction (please check):

☐ Patient

☐ Personal Representative (Print name legibly): _____

Please Sign:

_____ _____

Patient Personal Representative

_____ _____

Date Description of personal representative's authority to act for patient

We will provide you with a response to your request in a timely fashion in accordance with applicable law. We have the right in certain circumstances to deny access to all or part of the amendment you have requested.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

11. INDIVIDUAL'S REQUEST FOR AN ACCOUNTING OF DISCLOSURES

11.1 PURPOSE OF POLICY

To ensure compliance with the Privacy Rule's requirements regarding the Individual's right to receive an accounting of certain Disclosures of his or her own PHI.

11.2 POLICY DETAIL

An Individual has a right to receive an accounting of Disclosures of his or her own PHI made by Provider in the six years before the date on which the accounting is requested, except for Disclosures:

- to carry out Payment, Treatment and Health Care Operations (except that Disclosures from electronic records may have to be included in an accounting if and to the extent required by the HIPAA Rules);
- to individuals of PHI about them;
- pursuant to a proper authorization;
- to persons involved in the Individual's care or Payment for care;
- for national security or intelligence purposes;
- to correctional institutions or Law Enforcement Officials in custodial situations;
- that are part of a Limited Data Set;
- incident to a Use or Disclosure otherwise permitted or required by the Privacy Rule.

Depending on the compliance date Required by Law for a particular record or for electronic health records, individuals have a right to an accounting of Disclosures made for treatment, payment, or health care operations purposes for the previous three years. An Individual may request an accounting of Disclosures for a period of time less than six years from the date of the request. All requests for an accounting must be submitted in writing on the forms available from the Privacy Official.

All requests for an accounting must be submitted in writing on the forms available from the Privacy Official.

CONTENT OF THE ACCOUNTING. Provider will provide the Individual with a written accounting that meets the following requirements:

- The accounting must include Disclosures of PHI that occurred during the six years (or such shorter time period at the request of the Individual or if the request involves electronic health records) before the date of the request, including Disclosures to or by Business Associates of Provider. The Accounting will not include Disclosures made by Provider that occurred prior to the compliance date for Provider, or six years prior to the request, whichever is shorter.
- For each Disclosure, the accounting must include the following core elements:
  - The date of the Disclosure.
  - The name of the entity or person who received the PHI and, if known, the address of such entity or person.

- A brief description of the PHI Disclosed.
- A brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure, or, in lieu of such statement, a copy of a written request for Disclosure, if any.

MULTIPLE DISCLOSURES TO SAME PERSON OR ENTITY. If, during the period covered by the accounting, Provider has made multiple Disclosures of PHI to the same person or entity for a single purpose under the HIPAA Privacy Rule, the accounting may, with respect to such multiple Disclosures, provide:

- the core elements required to be in all accountings as described above for the first Disclosure during the accounting period;
- the frequency, periodicity, or number of the Disclosures made during the accounting period; and
- the date of the last such Disclosure during the accounting period.

TIMING OF PROVIDER'S RESPONSE. Provider must act on the Individual's request for an accounting no later than 60 days after receipt of such a request. In its response:

- Provider will provide the Individual with the accounting requested; and
- if Provider is unable to provide the accounting within the time required by the Privacy Rule, Provider may seek to extend the time to provide the accounting by no more than 30 days, provided that Provider, within the original 60-day time limit, gives the Individual a written statement of the reasons for the delay and the date by which Provider will provide the accounting. Provider will have only one such extension.

IMPOSING FEES FOR ACCOUNTING. Provider will provide the first accounting in any 12-month period ***without charge***. Provider may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same Individual within the same 12-month period, provided that Provider informs the Individual in advance of the fee and provides the Individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

TEMPORARY SUSPENSION OF RIGHT TO AN ACCOUNTING. Provider will temporarily suspend an Individual's right to receive an accounting of Disclosures to a Health Oversight Agency or Law Enforcement Official for the time specified by such agency or official, if such agency or official provides Provider with a written statement that such an accounting to the Individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the agency or official statement referenced in the preceding paragraph is made orally, Provider will:

- document the statement, including the identity of the agency or official making the statement;
- temporarily suspend the Individual's right to an accounting of Disclosures subject to the statement; and
- limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless the agency's or official's written statement is submitted during that time.

RETAINING DOCUMENTATION. Provider will document the following and retain the documentation for a period of six years:

- The information required to be included in an accounting of Disclosures of PHI.
- The written accounting that is provided to the Individual under this section.
- The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Form: Request for an Accounting or Disclosures of Medical Information

Patients or their personal representatives may receive a description of certain types of non-routine Disclosures of the patient's medical information made by [INSERT PROVIDER NAME]. This description is known as an "accounting." The right to an accounting comes from federal regulations called the HIPAA Privacy Rule. The HIPAA Privacy Rule permits you to request an accounting of certain non-routine Disclosures of medical information that may have occurred up to 6 years prior to the date on which the accounting is requested. Beginning on January 1, 2011 or January 1, 2014, depending on the compliance date required by law for a particular record, for electronic health records, individuals have a right to an accounting of Disclosures made for treatment, payment or health care operations purposes for the previous three years.

To assist us in responding to your request, please fill out the following information:

Patient's Name (Please print legibly): _____

Patient's Mailing Address

Street: _____

City: _____ **State:** _____ **Zip Code:** _____

Patient's Date of Birth (mm/dd/yyyy) _____/_____/_____

Time Period of the Accounting Request: (please check one)

☐ The time period between the following dates (but not greater than 6 years, or 3 years for certain routine Disclosures of electronic health records).

From _____ to _____.

Person Requesting accounting: (please check one):

☐ Patient

☐ Personal representative (Print name legibly):_____

Attach a copy of the documentation that establishes you as the patient's personal representative under state law.

Signature of patient OR patient's personal representative:

_____	_____
Patient	Patient's Personal Representative
_____	_____
Date	Description of personal representative's authority to make medical decisions for patient

We will provide you with a response to your request in a reasonable time period, in accordance with applicable law.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

12. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

12.1 PURPOSE OF POLICY

To ensure that individuals are free to exercise their rights under the Privacy Rule without intimidation or coercion.

12.2 POLICY DETAIL

Provider may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against the Individual or another person for:

- filing of a complaint with the Secretary;
- testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing; or
- opposing any act or practice made unlawful by the Privacy Rule, provided the Individual or other person has a good faith belief that the practice proposed is unlawful and the manner of opposition is reasonable and does not involve a Disclosure of PHI in violation of the Privacy Rule.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

13. WAIVER OF RIGHTS

13.1 PURPOSE OF POLICY

To ensure compliance with the Privacy Rule or other applicable law regarding an Individual's waiver of his or her rights regarding his or her PHI.

13.2 POLICY DETAIL

Provider may not seek or request that an Individual waive any right, in part or in whole, provided under the Privacy Rule, or other applicable law, regarding the confidentiality of medical information or the confidentiality of information pertaining to the payment for health care, as a condition for receiving treatment from Provider.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

14. DOCUMENTATION REQUIREMENTS AND RETENTION OF RECORDS

14.1 PURPOSE OF POLICY

To ensure compliance with the Privacy Rule regarding documentation requests and the retention of records.

14.2 POLICY DETAIL

POLICIES AND PROCEDURES. Provider will maintain in written or electronic form all policies and procedures implemented with respect to PHI and all documents required to be maintained by the Privacy Rule.

COMMUNICATIONS. If a communication document or record is required by Provider to be in writing, Provider will maintain such writing, or an electronic copy of that writing, as documentation.

WRITTEN OR ELECTRONIC RECORD. If an action, activity or designation is required to be documented, Provider will maintain a written or electronic record of the action, activity or designation. If records are retained in electronic form, Provider will ensure that:

- the record keeping system has reasonable controls designed to ensure the integrity, accuracy, authenticity and reliability of the electronic records;
- the electronic records are maintained in reasonable order, in a safe and accessible place and are capable of being readily inspected and examined;
- the electronic records are readily convertible into legible paper copies; and
- adequate records management systems are established and implemented to ensure that documents are labeled adequately and stored securely, back-up electronic copies are made and paper copies are kept for records that cannot be clearly, accurately and completely transferred to electronic media.

DOCUMENTS PROVIDER MUST RETAIN. Provider will retain the following documents:

- Provider's Notice of Privacy Practices that are issued to individuals.
  Accounting of Disclosures Log
- Individual authorizations.
- Individuals' Designated Record Sets.
- Copies of these policies and procedures.
- Workforce Member Training Documentation and Logs
- Individual complaints and their outcomes.
- Records of any sanctions imposed in connection with non-compliance with HIPAA.
- Records of any PHI Used or Disclosed for research purposes, as allowed without authorization
- Copies of Individual requests for restrictions on the Use and Disclosure of their PHI and Provider's responses.
- Copies of Individual requests for confidential communications and Provider's responses.
- Copies of Individual requests for a written accounting of Disclosures and Provider's responses.

- Copies of any Business Associate Agreements entered into by Provider.

PERIOD OF DOCUMENT RETENTION. Provider will retain any documentation required to be retained under HIPAA for a period of six years from the date of its creation, or the date when it was last in effect, whichever is later.

DOCUMENT DESTRUCTION. If Provider does not need to retain a record or document, the record or document will be disposed of in a manner that will not permit any PHI contained in the record or document to be Disclosed. Destruction of documents or records stored in electronic media must ensure that the data is wiped from electronic media so that it cannot be recovered. **Documents that are relevant to pending litigation or government investigations must not be destroyed**.

- If the document or record has been maintained in a paper format, the paper will be shredded or burned, or Provider will Use some other feasible method that will prevent the reconstruction of the data.
- If the document or record has been received in an electronic format, any hardware on which the record was saved will be wiped clean before the hardware is sold, reviewed, or destroyed.
- Any electronic media containing PHI will be wiped clean to ensure that even deleted items containing PHI are eliminated and cannot be re-created before the media is re-Used.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

15. AUTHORIZATIONS

15.1 PURPOSE OF POLICY

To ensure that all requested Disclosures, other than to the Individual whose PHI is being Disclosed, that are not either required or permitted under the Privacy Rule are made pursuant to a valid authorization.

15.2 POLICY DETAILS

Individuals may expressly authorize Disclosures of their PHI, and an authorization will be obtained for Uses and Disclosures of PHI not otherwise permitted by law or these policies. For example, PHI will not be Used for marketing, as that term is defined in the HIPAA Rules, without the Individual's authorization, unless otherwise permitted by the HIPAA Rules. Before disclosing any PHI pursuant to an authorization, Workforce Members should verify that the authorization form is valid. Compound authorizations (authorizations that are combined with a document that includes written permission relating to some other topic) are impermissible in many situations. Valid authorization forms must meet the following requirements:

- Be properly signed and dated by the Individual or the Individual's personal representative. If signed by a personal representative, a brief description of the personal representative's authority to make the authorization will also be required.
- Be written in plain language.
- Have a specific date or event upon which the authorization will terminate and that date or event, to the knowledge of Provider, must not have already occurred.
- Not, to the knowledge of Provider, have been revoked by the Individual.
- Contain a description of the information to be Used or Disclosed that identifies it in a meaningful and specific way.
- Contain the name or other specific identification of the person, class of persons or entity authorized to Use or Disclose the PHI.
- Contain the name or other specific identification of the person, class of persons or entity to whom Provider may Disclose the PHI.
- Contain a description of the purpose for each Disclosure.
- Contain a statement about the Individual's right to revoke the authorization, the procedures for revoking the authorization and a statement that the revocation is not applicable to Disclosures made by Provider in reliance on the authorization.
- Contain a statement about the possibility that the PHI that will be Disclosed pursuant to the authorization may be re-Disclosed by the recipient, subject to limitations specified in the *Part 2 Policy*.
- Contain a statement that Provider may not condition an Individual's enrollment or eligibility for benefits on an authorization requested by Provider.
- All Uses and Disclosures made pursuant to an authorization must be consistent with the terms and conditions set forth in the authorization.
- All individuals should receive a copy of any authorization that Provider requests the Individual to sign.

15.3 CALIFORNIA REQUIREMENTS

Abortion Information disclosed outside California:

Provider must obtain an authorization to disclose, transmit, transfer, share, or grant access to medical information in the EHR system or through a health information exchange (HIE) that would identify an individual and that is related to an individual seeking, obtaining, providing, supporting, or aiding in the performance of an abortion that is lawful under the laws of this state when the disclosure is to any individual or entity from another state.

- Authorization must clearly state that medical information on abortion or abortion-related services may be disclosed, and only to the extent and for the purposes expressly stated in the authorization.
- No authorization is required for disclosure
    - for payment permitted without authorization to the extent recipient agreements not to further disclose the information in a way that would violate this specific California law (Cal Civ. Code 56.110(a)).
    - for peer review, accreditation, or reviewing health care services with respect to medical necessity, level of care, quality of care, or justification of charges
    - for bona fide research purposes; IRB should consider the potential harm to patient and patient's privacy when the research uses data that contains information related to abortion or abortion-related services and the research is performed out of state.

Gender Affirming Care:

Provider shall not release medical information related to a person or entity otherwise authorized to receive medical information when the information concerns an individual seeking or obtaining gender-affirming health care or gender-affirming mental health care or to a person or entity allowing a child to receive gender-affirming health care or gender-affirming mental health care when the information and is requested pursuant to another state's law that authorizes a person to bring a civil or criminal action against a person or entity that provides, seeks, obtains, or receives gender-affirming health care or gender-affirming mental health care or who allows a child to receive gender-affirming health care or gender-affirming mental health care.

Immigration Enforcement:

Provider may not disclose medical information for immigration enforcement without the patient's authorization. No authorization is required for disclosure as permitted for treatment, payment, or healthcare operations, county coroner, medical examiner or forensic pathologist, bona fide research purposes, organ donor, adverse event reporting to the FDA, and other purposes under Cal. Civ. Code 56.10 (c).

Genetic Test Results:

Provider must obtain an authorization to disclose to a third party the results of genetic testing that include individual identifying information. The individual must be given a copy of the authorization.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

16. PERMITTED DISCLOSURES OF PHI

16.1 PURPOSE OF POLICY

To ensure that Provider only Discloses an Individual's PHI to family members and close friends in appropriate circumstances and does not improperly Disclose an Individual's PHI, and to enable PHI to be included in the facility directory.

16.2 POLICY DETAILS

Generally, Provider will not Disclose an Individual's PHI to third parties, except as required or permitted under the Privacy Rule or as expressly authorized by the Individual. Provider may, however, allow Disclosures to family members and close friends who are involved in the Individual's care or payment for the Individual's care, and Provider may do so only after the Individual is aware that such Disclosures may be made, has had an opportunity to object to Provider's making such Disclosures and has failed to object. If the Individual does not object, or in emergency circumstances and in a manner consistent with the Individual's best interest and any prior expressed preference, Provider may Use the following PHI to maintain a directory of individuals in the facility: name; location in the facility; general condition that does not communicate specific medical information; and religious affiliation.

Provider may also Disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the Disclosures allowed by the HIPAA Rules in situations where, in the exercise of professional judgment, the Provider determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

16.2.1 WHEN INDIVIDUAL IS UNAVAILABLE.

If the Individual is not present, or the opportunity to agree or object to the Use or Disclosure cannot practicably be provided because of the Individual's incapacity or an emergency circumstance, the Covered Entity may, in the exercise of professional judgment, determine whether the Disclosure is in the best interests of the Individual and, if so, Disclose only the PHI that is directly relevant to the person's involvement with the Individual's care or payment related to the Individual's health care or needed for notification purposes. A

Covered Entity may Use professional judgment and its experience with common practice to make reasonable inferences of the Individual's best interest in allowing a person to act on behalf of the Individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

If the Individual is not present and Provider needs to convey messages of a time sensitive or urgent nature, Provider may leave voicemail messages or messages with persons answering the Individual's phone containing PHI under the following circumstances:

- Provider Workforce Member leaving the message confirms that it is the most recent phone number provided by the Individual.

- The Individual has not instructed Provider to refrain from leaving detailed messages or has not requested that Provider communicate only through an alternative method.

- Including PHI in the messages is necessary and in the Individual's best interest in, the Workforce Member's professional judgment. For example, if the Individual requires urgent treatment, the Workforce Member may determine that the Individual needs to receive that information as soon as possible and leaving a voicemail or other message is a prudent way to convey that information quickly.

- The PHI Disclosed in the message is as limited as is feasible and is the minimum amount of PHI necessary. Generally, Provider would only leave a name and number and a request to call back. However, there are certain situations where the message must contain more detailed information. The message should not contain unnecessary PHI or Disclose particularly sensitive conditions (such as cancer, HIV, sexually transmitted infections, mental health conditions, or pregnancy).

OBJECTIONS TO DISCLOSURES. Provider will provide individuals with a Notice of Privacy Practices generally describing the types of Disclosures that may be made to friends and family. If the Individual is present when Provider wishes to Disclose to friends and/or family, the Individual will be given an opportunity to object. Except in emergencies, individuals must be given an opportunity to object to being included in the directory. Notwithstanding the foregoing, Provider will comply with state law requirements that are stricter or in addition to HIPAA or Part 2 requirements (and not preempted by such federal laws) related to disclosing PHI to friends and family and inclusion in the facility directory.

16.2.3 VERIFICATION.

Except for requests for directory information from the clergy or from people who ask for an Individual by name, if a Workforce Member receives a request for Disclosure from an Individual claiming to be an individuals' spouse, other family member, close friend, or personal representative, the Workforce Member must seek to verify that person's identity as set forth in the *Verification of Persons Requesting PHI Policy*. Once the identity of the person has been established, the Workforce Member should check the Individual's Designated Record Set to determine if this Individual is one that the Individual has objected to being the recipient of his or her PHI. If no written objection to such Disclosure is in the Designated Record Set, the Workforce Member may make the Disclosure. If the Workforce Member is unable to verify the identity of the Individual, or the Individual objected to Disclosure of his or her PHI to that Individual, then no Disclosure will be made unless the Individual expressly authorizes it. If a Workforce Member is uncertain about any of these matters, he or she should contact the Privacy Official.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

16.2.4 SUBPOENAS, COURT-ORDERS, AND WARRANTS

Provider may Use and Disclose PHI in compliance with and as limited by:

- A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
- A grand jury subpoena; or
- An administrative request, including an administrative subpoena or summons, or a civil or an authorized investigative demand or similar process, provided that: The information sought is relevant and material to a law enforcement inquiry; The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which information is sought; and De-Identified Information could not reasonably be Used.

In all cases where Disclosure is required by subpoena or other process, Provider must ensure that the subpoena or other legal process has been validly executed, and the Disclosure strictly complies with the terms of the subpoena, including scope of the information Disclosed, method of Disclosure (e.g., written documents), whether Provider has received "satisfactory assurances" that notice of the subpoena was provided in writing to the Patient, and the timing for Disclosure. If the subpoena, order or warrant only requires Disclosure of written items, Provider should not Disclose the information orally. If the subpoena requires Disclosure at a specific time, Provider should not Disclose the information before the deadline without the patient's consent. Documentation must include a statement that written notice was provided to the Individual who is the subject of the subpoenaed records.

Provider should maintain a copy of the subpoena, order or warrant, and document the facts of the Disclosure in the Accounting of Disclosures Log.

When producing records:

- DO NOT deliver prior to date indicated on the subpoena; the Patient has the right to object and may do so up documents are due
- DO limit to specific records requested
- DO maintain a description of records delivered; Accounting of Disclosures Log must be completed and included in the patient record
- DO deliver by secure electronic method if requested
- DO deliver by USPS certified mail with return receipt requested, FedEx, UPS, or by delivery in person; maintain records of delivery

The Privacy Officer shall contact the Vice President of Clinical Services and Compliance and Provider's legal counsel if questions arise regarding Disclosures of PHI pursuant to any legal process.

CALIFORNIA RESTRICTIONS ON SUBPOENA RESPONSES

ABORTION: Provider shall not release medical information that would identify an individual or that is related to an individual seeking or obtaining an abortion to law enforcement unless the release is pursuant to a subpoena that is not based on another state's laws that interfere with a person's rights to reproductive

health care under California laws. Provider shall not cooperate with any inquiry or investigation by, or provide medical information to, any individual, agency, or department from another state or, to the extent permitted by federal law, to a federal law enforcement agency that would identify an individual and that is related to an individual seeking or obtaining an abortion or abortion-related services that are lawful under the laws of this state.

Consultation with legal counsel is required prior to response.

16.2.5 DISCLOSURE RELATED TO VICTIMS OF ABUSE, NEGLECT, OR DOMESTIC VIOLENCE.

Provider will Disclose PHI about a Patient who Provider reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority authorized by law to receive such reports:

- To the extent it is required by law;
- To the extent it is authorized by the Patient; or
- To the extent it is permitted by law and either: Provider believes that the Disclosure is necessary to prevent harm to the Patient or other potential victims; or if the Patient is incapable of agreeing, a government authority represents that PHI is not intended to be Used against the Patient and an immediate enforcement activity would be materially adversely affected by waiting.

Workforce Member will inform the Patient that Provider made the Disclosure unless:
- Informing the Patient would place the Patient at risk of serious harm; or
- The person that Provider would be informing of the Disclosure is the Personal Representative of the Patient, the Personal Representative is likely responsible for the abuse, neglect, or other injury, and informing the Personal Representative is not in the best interest of the Patient.

16.2.6 DISCLOSURE REQUIRED BY LAW.

As Required by Law, including such laws as those that require the reporting of certain types of wounds or other physical injuries, except for laws regarding the reporting of child abuse or neglect or reports about abuse, neglect, or domestic violence.

16.2.7 DISCLOSURE TO IDENTIFY OR LOCATE A SUSPECT, FUGITIVE, MATERIAL WITNESS, OR MISSING PERSON.

The following PHI may be Disclosed pursuant to a Law Enforcement Official's request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person:
- Name and address;
- Date and place of birth;
- Social security number;
- ABO blood type and Rh factor;
- Type of injury;

- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

Provider may not, however, Disclose PHI relating to a Patient's DNA or DNA analysis, dental records, typing, samples, or analysis of body fluids or tissue.

16.2.8 DISCLOSURE RELATED TO VICTIMS OF A CRIME.

Provider may Disclose PHI in response to a Law Enforcement Official's request for information about an Patient who is suspected to be a victim of a crime, other than Disclosures made for public health activities or Disclosures about victims of abuse, neglect of domestic violence, if:

- The Patient agrees to the Disclosure; or
- Provider is unable to obtain the Patient's agreement because of incapacity or other emergency circumstance, provided that the Law Enforcement Official represents that:
  - The information is needed to determine whether a violation of the law by a person other than the Patient has occurred;
  - PHI is not intended to be Used against the Patient;
  - The immediate law enforcement activity that depends upon the Disclosure would be materially and adversely affected by waiting until the Patient is able to agree to the Disclosure; and
  - Practice determines that the Disclosure is in the best interests of the Patient.

16.2.9 DISCLOSURE TO REPORT SUSPICIOUS DEATH.

To alert law enforcement of the death of a Patient if Provider has a suspicion that death may have resulted from criminal conduct.

16.2.10 DISCLOSURE OF EVIDENCE OF A CRIME ON THE PREMISES.

If Provider believes, in good faith, PHI to be Disclosed constitutes evidence of a crime that occurred on the premises of Provider.

16.2.11 DISCLOSURE RELATED TO CRIMES AGAINST WORKFORCE MEMBERS.

Provider shall assess the Disclosure to determine whether the Workforce Member has a good faith belief that PHI to be Disclosed constitutes evidence of a crime on the premises and whether the:

- PHI is about the suspected perpetrator of the criminal act; and
- Workforce Member who is a victim of a crime only Disclosed the following information about the suspect:
  - Name and address;
  - Date and place of birth;
  - Social Security number;

- ABO blood type and Rh factor;
- Type of injury treated by Provider;
- Date and time of treatment;
- Date and time of death, if applicable; and
- Distinguishing characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

If a Workforce Member who is a victim of a crime Disclosed PHI but did not meet all of the requirements above, Practice may sanction Workforce Member.

16.2.12 DISCLOSURE RESULTING FROM OFF-PREMISE MEDICAL EMERGENCY

If any physician of Provider provides emergency health care in response to a medical emergency, other than an emergency on the premises of Provider, then Provider may Disclose PHI to a Law Enforcement Official if the Disclosure is necessary to alert law enforcement as to:

- The commission and nature of a crime;
- The location of a crime of the victim(s) of a crime; and
- The identity, description, and location of the perpetrator of a crime.

If the medical emergency described in this paragraph is a result of abuse, neglect, or domestic violence, then this paragraph does not apply and Provider will adhere to the Victims of a Crime paragraph under this Policy.

16.2.13 DISCLOSURE TO PUBLIC HEALTH AUTHORITIES

Provider may Disclose PHI to an entity authorized by law to conduct certain public health activities, e.g., to report certain communicable diseases or immunizations or report child abuse or neglect.

16.2.14 DISCLOSURE TO HEALTH OVERSIGHT AUTHORITIES

Provider may Disclose PHI to a health oversight agency (e.g., state licensing boards, HHS, CMS, OIG, etc.) for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight. A health oversight activity does not include an activity where the Patient is the subject of the activity and the activity is not directly related to: the receipt of health care, a claim for public benefits related to health; or qualification for, or receipt of, public benefits or services when the Patient's health is integral to the claim.

16.2.15 DISCLOSURE TO IDENTIFY OR APPREHEND CRIMINAL SUSPECT

Provider may Disclose PHI necessary for Law Enforcement Officials to identify or apprehend an Individual because of a statement by an Individual admitting to participation in a violent crime that Provider reasonably believes may have caused serious physical harm to the victim; or where it appears from all the

circumstances that the Individual has escaped from a correctional institution or from lawful law enforcement custody. Provider may only Disclose the following to Law Enforcement pursuant to this paragraph:

- The statement admitting participation in a violent crime (see above);
- The name and address of the Patient;
- The date and place of birth of the Patient;
- The Social Security number of the Patient;
- ABO blood type and Rh factor of the Patient;
- The type of injury Provider treated;
- The date and time of treatment;
- The date of death, if applicable; and
- A description of distinguishing characteristics including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

Provider may not, however, Disclose PHI relating to an Patient's DNA or DNA analysis, dental records, typing, samples, or analysis of body fluids or tissue.

Provider may NOT Use or Disclose PHI, as contemplated under this paragraph, if the information is learned by Provider in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the Disclosure, or counseling or therapy; or through a request by the Individual to initiate or to be referred for the treatment, counseling, or therapy.

16.2.16 DISCLOSURE TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

Provider may Disclose only necessary PHI to law enforcement, family members of the patient, or other persons, when Provider believes the patient present a serious and imminent threat to self or others. Provider must believe in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others. Provider, consistent with applicable state and federal law and standards of ethical conduct, may alert those persons whom the provider believes are reasonably able to prevent or lessen the threat. For example, if a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, the mental health professional may alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat. Provider may consult with legal counsel or Privacy Officer.

16.2.17 REFERENCE TO OTHER USE AND DISCLOSURE POLICIES

- **FUNDRAISING.** Provider may Use or Disclose PHI for fundraising purposes as provided in the *Fundraising Policy*.

- **PUBLIC OFFICIALS**. Provider may Use or Disclose PHI to Public Officials in accordance with the *Requests by a Public Official Policy*.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

- **SUBSTANCE USE DISORDER RECORDS**. Use or Disclosure of Substance Use Disorder Records must comply with requirements in the *Part 2 Policy* to this *HIPAA Policy Manual*.

    - **Non-Part 2 Programs**. Providers that *receive* Substance Use Disorder Records must also comply with certain requirements in the *Part 2 Policy* related to Redisclosure.

        - Redisclosure by a Non-Part 2 Program. To the extent that Provider's non-Part 2 Program facility receives SUD Records with a notice not to re-Disclose such information, Provider shall comply with such notice. Provider may seek legal consultation if questions arise regarding Redisclosure of SUD Records. If Provider receives SUD Records based on a single consent for all treatment, payment, and health care operations, then Provider is not required to segregate or segment such Records.

        - Documentation of SUD treatment by a Non-Part 2 Program. The act of recording information about a SUD and its treatment by Provider or its Workforce Members as non-Part 2 Program facility (which is not subject to 42 C.F.R. Part 2) does not by itself render a medical record subject to the restrictions under the *Part 2 Policy*.

17. DISCLOSURES TO BUSINESS ASSOCIATES

17.2 PURPOSE OF POLICY

To ensure that Workforce Members properly Disclose Individual PHI to Business Associates of Provider.

17.3 POLICY DETAILS

All Disclosures to and Uses and Disclosures by a Business Associate of Provider must be made in accordance with a valid written Business Associate agreement. Before disclosing PHI to a Business Associate, Provider's Workforce Members must determine that a valid Business Associate agreement is in place. The Business Associate agreement must comply with the Security Rule and Privacy Rule. In addition:

- all Disclosures must be consistent with the terms of the Business Associate agreement;
- Disclosures must comply with the Minimum Necessary Standard; and
- Disclosures that must be accounted for must be documented in accordance with *the Documentation Requirement and Record Retention Policy*.

18. DE-IDENTIFIED INFORMATION AND LIMITED DATA SETS

18.2 PURPOSE OF POLICY

To clarify when health information is de-identified and is, therefore, not subject to HIPAA and the Privacy Rule.

18.3 POLICY DETAILS

De-identified information is health information that does not identify an Individual or with respect to which there is no reasonable basis to believe that the information can be Used to identify an Individual. There are two ways Provider can determine that health information is de-identified.

REMOVE IDENTIFIERS. The first way to de-identify health information is by removing the following 18 specific identifiers of the Individual or of relatives, employers, or household members of the Individual:

- Names.
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an Individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

- Telephone numbers.
- Fax numbers.
- Electronic mail addresses.
- Social Security number.Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic, or code, except as permitted by this section.

Also, Provider must not have actual knowledge that the information could be Used alone or in connection with other information to identify an Individual who is a subject of the information.

RETAIN EXPERT. The second way to de-identify health information is to retain a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable and have that person determine that the risk is very small that the information being Disclosed could be Used, or in combination with other reasonably available information, by an anticipated recipient to identify the Individual who is the subject of the information and the expert documents the methods and results of the analysis that justified his or her conclusions.

LIMITED DATA SETS. Information that has been stripped of many of the 18 identifying factors may still remain PHI. Nevertheless, the stripped down information may be Disclosed if the information is part of a Limited Data Set and is Used and Disclosed only pursuant to a Data Use Agreement.

APPROVAL FROM PRIVACY OFFICIAL REQUIRED. Any Workforce Member who is asked to Disclose de-identified information, summary health information, or a Limited Data Set should first obtain approval from the Privacy Official for the Disclosure. The Privacy Official will verify that the information is de-identified or is part of a Limited Data Set, and that the conditions allowing for Disclosure have been met. Once information has been verified as having been de-identified, it may be freely Used or Disclosed. De-identified information is not PHI and is not subject to HIPAA or the Privacy Rule. A Limited Data Set is still PHI and is subject to the provisions of a Data Use Agreement

19. CALIFORNIA RESTRICTIONS: INFORMATION REGARDING GENDER AFFIRMING CARE, ABORTION AND ABORTION-RELATED SERVICES AND CONTRACEPTION

19.1 PURPOSE OF POLICY

To clarify when certain sensitive health information maintained electronically in an electronic health records system is further protected by California law.

19.2 INFORMATION PROTECTED

Medical information related to gender affirming care, abortion and abortion-related services, and contraception is considered Sensitive Medical Information afforded protections that are in addition to the privacy protections under HIPAA. "Gender affirming care" means “Gender affirming health care” and “Gender affirming mental health care” as defined below. “Gender affirming health care” means medically necessary health care that respects the gender identity of the patient, as experienced and defined by the patient, and may include, but is not limited to, the following: (i) Interventions to suppress the development of endogenous secondary sex characteristics. (ii) Interventions to align the patient’s appearance or physical body with the patient’s gender identity. (iii) Interventions to alleviate symptoms of clinically significant distress resulting from gender dysphoria, as defined in the Diagnostic and Statistical Manual of Mental Disorders, 5th Edition. “Gender affirming mental health care” means mental health care or behavioral health care that respects the gender identity of the patient, as experienced and defined by the patient, and may include, but is not limited to, developmentally appropriate exploration and integration of identity, reduction of distress, adaptive coping, and strategies to increase family acceptance.

.

19.3 ACCESS RESTRICTIONS/DATA SEGREGATION

User access privileges to Sensitive Medical Information must be limited to those persons who are authorized to access specified medical information.

Provider must prevent disclosure, access, transfer, transmission, or processing of Sensitive Medical Information to persons outside of the state of California.

Provider must segregate Sensitive Medical Information from the rest of the patient’s record and automatically disable access to segregated Sensitive Medical Information by individuals and entities in another state.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

20. COMPLAINTS

20.1 PURPOSE OF POLICY

To set forth Provider's procedures for receiving and responding to complaints, questions, or inquiries about Provider's privacy practices or the Use or Disclosure of PHI in the course of providing services.

20.2 POLICY OF DETAILS

Individuals or Workforce Members may file complaints about alleged violations of these policies and procedures or alleged violations of HIPAA. If someone wants to file a complaint, they will be asked to submit their complaint to the Privacy Official in writing. If the Individual refuses to submit the complaint in writing, the Workforce Member receiving the complaint should document the details in writing and forward the documentation to the Privacy Official.

WRITTEN ACKNOWLEDGEMENT. Upon receipt of an inquiry or question, the Privacy Official will make reasonable efforts to respond in writing to the Individual within 15 calendar days of receipt of the inquiry. The Privacy Official may consult with the Security Official, Provider's legal counsel, and/or Vice President of Clinical Services and Compliance, as needed during his or her evaluation of any inquiry or question. If the Privacy Official is unable to provide a reasonably accurate answer within that time period, the Privacy Official should request any information not originally provided which would be needed from the Individual to provide an adequate answer. If the Privacy Official is able to answer the inquiry or question, the written response should contain the appropriate answer.

PRIVACY OFFICIAL'S INVESTIGATION. If necessary following the initial response, the Privacy Official will undertake an investigation which will, if practicable, be completed within 30 calendar days of the complaint. If the Privacy Official in his/her sole discretion believes that additional time is needed, he or she may take the time needed to complete the investigation. The Privacy Official may consult with the Security Official, Provider's legal counsel, and/or Vice President of Clinical Services and Compliance, as needed during his or her evaluation. Upon completion of the investigation, the Privacy Official will inform the Individual of the results of his/her investigation and the action taken to address the subject matter of the complaint, if any.

DOCUMENT RETENTION. Complaints, the Privacy Official's initial response, the Privacy Official's request for an extension and the Privacy Official's response following an investigation (if any) will be retained by the Privacy Official in accordance with *Provider's Documentation Requirements and Retention of Records Policy.* A copy of this complaint policy will be made available to any Individual upon that Individual's request.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

21. DESIGNATED RECORD SETS

21.1 PURPOSE OF POLICY

To set forth the scope of an Individual's Designated Record Set

21.2 POLICY DETAILS

An Individual's Designated Record Set with respect to Provider consists of the following records containing an Individual's PHI if kept in the Individual's paper or electronic file:

- All claims or billing records submitted to and/or maintained by Provider.
- Medical records.
- Enrollment, payment, claims adjudication and case or medical management records or record systems maintained by Provider.
- An Individual's written communications to Provider, written communications about the Individual or communications that were written on behalf of the Individual, and written communications from Provider, or an insurer or HMO providing benefits, concerning the Individual.
- Summaries, notes or logs of telephonic communications to Provider by the Individual or concerning the Individual, but only if Used to make decisions about Individual

The Designated Record Set does not include the following:

- PHI stored in locations where the PHI is also available in other sources, or PHI included in records not focused on a specific Individual. This includes, but is not limited to, PHI stored in personal portable devices, hard drives, copy machines, fax machines, calendars, and employment files.
- Workforce Members' notes, if Used only to assist the Workforce Member in recalling information or for other purposes and not Used to make decisions about the Individual, or notes that are incorporated into other records, such as electronic medical record.
- Correspondence or communication from Individual if not Used to make decisions about Individual, even if correspondence or communication contains PHI.
- Financial reports and accounting records.
- Separately maintained psychotherapy notes.
- Records of internal access to PHI.
- Requests for access, amendments and accountings of Disclosures made by an Individual and Provider's responses.
- Complaints filed by an Individual and the Privacy Official's responses.

If there is any uncertainty about whether a particular document or record is part of an Individual's Designated Record Set, the final determination will be made by the Privacy Official. The Privacy Official may consult the Vice President of Clinical Services and Compliance and/or Provider's legal counsel.

For purposes of this policy, the term "record" means any item, collection, or grouping of information that includes PHI, and is maintained, collected, Used or disseminated by or for Provider.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

22. DESIGNATED PERSONNEL/ACCESS PROFILES

22.1 PURPOSE OF POLICY

To ensure that appropriate personnel or offices are designated to carry out certain functions and responsibilities.

22.2 POLICY DETAIL

HIPAA requires documentation of the people or offices responsible for specific activities related to compliance with HIPAA.

PRIVACY OFFICIAL.[*Insert Individual's title***]** is named as the Privacy Official for purposes of Provider's *HIPAA Policy Manual* and the federal privacy regulations. The Privacy Official may designate duties or obligations to Workforce Members as needed.

SECURITY OFFICIAL. .[*Insert Individual's title***]** is designated the Security Official for purposes of Provider's *HIPAA Policy Manual* and the federal security regulations. The Security Official may designate duties or obligations to Workforce Members as needed.

CONTACT OFFICE FOR QUESTIONS AND COMPLAINTS. The Privacy Official is the contact to receive questions and complaints, both from individuals and Workforce Members, regarding HIPAA or the privacy of PHI. The Privacy Official may designate others to assist with handling complaints. If a Workforce Member receives a complaint, the Workforce Member should forward the complaint to the Privacy Official, or his or her designee, for handling.

The Security Official is the contact to receive questions and complaints, both from individuals and Workforce Members, regarding security of ePHI. For cybersecurity issues contact the Security Official and report threats, suspicious emails, suspected breaches, and unusual activity to _____. If there is an urgent cybersecurity issue, call_____.

ACCESS PROFILES FOR WORKFORCE. Access privileges for Individual Workforce Members will be terminated or changed in conjunction with the termination of employment, contract, or change of level of access required. The IT Group will audit the access privileges in accordance with the *Administrative, Technical and Physical Privacy and Security Safeguards Policy* and shall report to Security Official and/or Privacy Official if any changes are needed.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

23. STATE LAW COMPLIANCE

23.1 PURPOSE OF POLICY

The purpose of this policy is to provide that Provider will abide by applicable state laws relating to the privacy and security of PHI, to the extent not preempted by HIPAA.

23.2 POLICY DETAIL

Provider will comply with both HIPAA and applicable state law not preempted by HIPAA. Provider has developed its Notice of Privacy Practices, which may be found on the Provider's website, to contain provisions to comply with state law. When it is impossible to comply with both state law and HIPAA, the HIPAA rules preempt state law except when the state law is more stringent or when the government has exempted a particular state law from preemption.

HIPAA does not preempt state laws that require using PHI to make certain reports regarding child abuse and neglect, certain infectious diseases, particular public health reporting, reporting for death certificates, and certain other mandated reports.

Provider will comply with HIPAA and related state laws and will follow state privacy and data breach laws as they relate to any potential HIPAA incident. For example, if a breach involves a social security number, driver's license number, or certain other information covered by state data breach laws, Provider will determine whether state law imposes more stringent or different requirements, such as a shorter time frame for reporting data breaches, Provider will comply with the timeframes set forth in the applicable state law.

23.3 PROCEDURAL GUIDANCE

Particular state law questions or questions of applicability regarding HIPAA or Part 2 shall be promptly referred to the Vice President of Clinical Services and Compliance and/or Provider's legal counsel for guidance and compliance.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

24. USE AND DISCLOSURE OF PSYCHOTHERAPY NOTES

24.1 BACKGROUND

Psychotherapy notes have a special definition under HIPAA, set forth below. They are given special protection regarding their Use and Disclosure.

> *"Psychotherapy notes"* mean notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and **that are separated from the rest of the Individual's medical record**.
>
> Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

24.2 POLICY

Provider recognizes that psychotherapy notes need to be handled separately and with additional protections regarding their Use and Disclosure. The general policy is that Provider will rarely, if ever, Use, Disclose, or possess psychotherapy notes. If Provider does need to Use or Disclose psychotherapy notes, the Privacy Official will consult legal counsel to ensure that the Use or Disclosure is consistent with state law and HIPAA.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

25. FUNDRAISING

25.1 PURPOSE OF POLICY

To ensure that Use and Disclosure of PHI for fundraising complies with the HIPAA Rules.

25.2 POLICY DETAIL

Provider may Use and Disclose to a business associate selected PHI for purposes of raising funds for Provider's own benefit without an Individual's authorization. However, an Individual does have the right to opt out of receiving such fundraising communications.
The following PHI may be Used for purposes of making fundraising communications:

- Demographic information relating to an Individual, including name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to an Individual;
- Department of service information;
- Treating physician;
- Outcome information; and
- Health insurance status.

Provider must include in any fundraising materials sent to an Individual a description of how the Individual may opt out of receiving any further fundraising communications. The opt out method must not cause the Individual to incur an undue burden or more than a nominal cost. Provider shall consider using a toll-free phone number, an email address, or similar methods that will provide an Individual with a simple, quick, and inexpensive way to opt out of receiving future fundraising communications. Provider shall not require individuals to write a letter to opt out of receiving future fundraising communications. Provider shall include in its Notice of Privacy Practices a statement that Provider Uses certain PHI in fundraising activities. Provider may not condition treatment or payment on the Individual's choice with respect to the recipient of fundraising communications. Further, Provider shall not send fundraising communications to any Individual who has elected not to receive such communications.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

26. SALE OF PROTECTED HEALTH INFORMATION

26.1 PURPOSE OF POLICY

To ensure that PHI is not sold except in strict compliance with the HIPAA Rules and other applicable law.

26.2 POLICY DETAIL

It is the policy of Provider not to engage in the sale of PHI without first obtaining the Individual's written authorization. For purposes of this policy, the sale of PHI means a Disclosure of PHI where the Provider directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI unless the Disclosure is for one of the following purposes:

- For public health purposes;
- For research where the remuneration is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI;
- For treatment and payment purposes;
- For the sale, transfer, merger, or consolidation of all or part of the Provider and related due diligence;
- To or by a business associate or subcontractor for business associate activities that the business associate or subcontractor undertakes on behalf of the principal and the only remuneration is for the performance of such activities;
- To the Individual under the Individual rights to access and an accounting of Disclosures provisions of the HIPAA rules;
- For Disclosures required by law; or
- For any other purpose permitted by the HIPAA Rules, where the only remuneration received by the Provider is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

27. SOCIAL MEDIA POLICY

27.1 PURPOSE

Provider recognizes certain employees and other personnel have personal accounts on various social networking sites such as Facebook, Linked-In, Instagram, and Twitter, and may create or contribute to blogs and the like. Provider has developed this policy to communicate social media Use guidelines that are necessary to protect the legitimate business interests of Provider and the privacy interests of the individuals we serve. This Policy is not intended to interfere with your expression of opinions or statements regarding any group concerns pertaining to terms and conditions of your employment or those of other Provider Workforce Members, but we must Use reasonable measures to ensure the privacy of the individuals receiving services.

27.2 SCOPE OF POLICY

"Social Media" includes any online tool, accessed either through the Internet or application software, which allows Users to post content (text, photo, video or audio), respond to posted content and engage in conversation with other Users via content exchanges.

This policy applies to all Workforce Members. The policy applies on Provider property, at Provider worksites, while participating in Provider-sponsored events (on or off Provider property) or wherever and whenever a Workforce Member is performing a function of his or her job. This policy applies whenever an employee is using Provider-issued equipment or devices (such as cellular smart phones, computers or other electronic devices) or any internet or electronic communication or information systems provided or maintained by Provider. This policy also applies to certain off-duty social media Use by Workforce Member, regardless of whether the Workforce Member is using Provider equipment or systems.

Workforce Members have no right of privacy when using Provider equipment or its internet, communication or information systems. Accordingly, when using any of Provider's equipment or systems to post or access content on social media, Workforce Members should not expect any such content to be private or confidential.

27.3 WORK RELATED SOCIAL MEDIA USE AND SHARING

Provider maintains certain social media sites to promote its services. Only authorized Workforce Members may post to these sites. Workforce Members who have not received express authorization from their supervisor to post to Provider's social media sites should only post or comment on Provider's social media sites in a manner that is consistent with the provisions of this Policy. While Provider's Workforce Members are encouraged to share official Provider posts on their own personal social media site pages, Workforce Members should not post or comment about shared posts in any manner that may violate this Policy.

27.4 PERSONAL SOCIAL MEDIA USE

Workforce Members' *personal* Use of social media should generally occur during non-working time (*e.g.* authorized break times, meal periods and off-duty hours) and must not interfere with the work and productivity of the employee or other employees and must not preempt or disrupt any of Provider's business activities.

27.5 CONFIDENTIAL INFORMATION

When posting on social media sites, Workforce Members must not include any Provider or patient confidential or proprietary information. By way of example, confidential or proprietary information includes non-public information about Provider's finances, business plans or strategies, employees, and patients and prospective patients, and marketing and advertising plans. Confidential information does not include information about terms and conditions of employment (including wages or benefits) of other Workforce Members, unless the employee obtains this information as part of the Workforce Member's job duties or through unauthorized or unlawful access to Provider's records or other employees' private property.

27.6 PROTECTED HEALTH INFORMATION

HIPAA's prohibition against disclosing PHI concerning Patients applies to Workforce Members' activities on social media. Accordingly, Workforce Members must not post or otherwise transmit any information relating to patients on or through social media, except in sharing authorized posts from Provider's social media sites. Prohibited posts include, but are not limited to any patient's photograph, dates related to the patient (other than year), age, health condition, other personal characteristics, or anything that a reasonable person could consider to be abusive, embarrassing or demeaning to individuals we serve or their families. **This prohibition applies even if the post or transmission does not include the patient's name or a photograph of the patient's face. It also applies even if the purpose of the social media communication is to respond to patient complaints.** All employees are expected to be familiar with Provider's HIPAA compliance policies and to make sure their social media and other activities comply with HIPAA and state privacy laws.

27.7 OTHER PROHIBITED ACTIVITY

In addition to confidential information and protected health information, Workforce Members must not post or otherwise transmit:

- False or derogatory information or statements about Provider's leadership or personnel, services, patients, vendors or other third parties who conduct business with Provider;

- Statements about other individuals associated in any way with Provider that are intended to bully or degrade, or that reasonably could be viewed as vulgar, obscene, malicious, threatening, or intimidating. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that contribute to a hostile work environment or otherwise violate Provider's policies against discrimination or harassment;

- Photographs or videos of yourself or anyone else in any patient care areas of Provider, or anywhere else on Provider's property where the taking or display of the photograph or video could negatively impact patient care or Disclose or contain PHI regarding any patient, or otherwise violate the privacy of any individuals associated in any way with Provider;

- Any commercial Use of the trademark or copyright materials without the express written approval of Provider's Chief Marketing Officer in consultation with the Vice President of Clinical Services and Compliance; or

- Any link to the Provider's website without disclosing that the employee is employed by Provider.

Employees should also comply with Provider's reasonable requests that other specified topics not be discussed for confidentiality or legal compliance reasons.

27.8 VIOLATIONS

Employees who fail to comply with this policy may be subject to disciplinary or corrective action, up to and including discharge.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

PART 2 POLICY

SUBSTANCE USE DISORDER PROGRAM POLICIES AND PROCEDURES

POLICY PURPOSE:

To comply with 42 C.F.R. Part 2 requirements pertaining to the Use, Disclosure, and Acess to Substance Use Disorder records created, held, or maintained by Provider's Substance Use Disorder programs subject to 42 C.F.R. Part 2. Provider will comply with applicable state laws and HIPAA except to the extent that it is not possible to comply with Part 2 requirements and state law or HIPAA. In such instances, 42 C.F.R. Part 2 requirements shall govern. Provider will consult with legal counsel when questions arise regarding the applicability of 42 C.F.R. Part 2, HIPAA, or state law.

POLICY SCOPE:

This Part 2 Policy applies to:

- all Provider's Covered Programs in the Provider System and other providers in the system that receive and maintain Substance Use Disorder Patient Records as defined in Part 2.
- Records created, received or acquired by a Covered Program that identify the Covered Patient and Diagnosis, Treatment or referral for treatment in a Part 2 Program for the Covered Patient relating to a Substance Use Disorder. Records include paper and electronic records but do not include information conveyed orally by a Part 2 Program to a non-part 2 provider for treatment purposes with the consent of the patient even if reduced to writing by the non-Part 2 provider or information that is a summary created by the non-Part 2 provider of the information.
- The special restrictions and consent requirements of this Part 2 Policy apply to the Use and Disclosure of information identifying an Individual as a Covered Patient.

This Part 2 Policy outlines the restrictions on Use and Disclosure of Substance Use Disorder records that identify a specified patient as having or having had a Substance Use Disorder, and bars, among other things:

- The introduction into evidence of a Substance Use Disorder record or testimony in any criminal prosecution or civil action before a Federal or state court;
- Reliance on such record or testimony to inform any decision or otherwise be taken into account in any proceeding before a Federal, state, or local agency;
- The Use of such record or testimony by any Federal, state, or local agency for a law enforcement purpose or to conduct any law enforcement investigation, and
- The Use of such record or testimony in any application for a warrant, absent Patient consent or a valid court order in accordance with Part 2.

In the event of any conflict between this Part 2 Policy and the HIPAA Policy Manual, this Part 2 Policy governs as it relates to Provider's Substance Use Disorder treatment programs. **This Part 2 Policy does not apply to Provider's facilities that are not Part 2 Programs as defined hereunder.**

DEFINITIONS:
Except as otherwise stated, capitalized terms shall have the meaning set forth in Section 2.11 of Part 2. Terms not defined herein or Section 2.11 of Part 2 shall have the meaning set forth in the HIPAA Policy Manual, if defined therein.

Affiliate means any person or entity Controlling, Controlled by or under common Control with another person or entity.

Central registry means an organization which obtains from two or more member programs patient identifying information about individuals applying for withdrawal management or maintenance treatment for the purpose of avoiding an Individual's concurrent enrollment in more than one treatment program.

Control means the direct or indirect power to govern the management and policies of an entity; or the power or authority through a management agreement or otherwise to approve an entity's transactions (includes Controlled, Controlling).

Covered Information means any information, paper or electronic, whether recorded or not, created by, received, or acquired by a Covered Program relating to a Covered Patient's diagnosis, treatment or referral for treatment for a Substance Use Disorder. (e.g., patient records, billing information, emails, voice mails, and texts).

- Covered Information includes, without limitation, medical records maintained by a Covered Program or obtained from a Covered Program identifying an Individual as a Covered Patient except for information received by a non-Part 2 provider that is not retained by the non-Part 2 provider.
- A non-Part 2 provider may record the identity of a Covered Patient and summarize information about the Substance Use Disorder and treatment for its patient records. This is not considered a Redisclosure and the summary information is not covered by Part 2 or subject to restriction on Redisclosure by Part 2.
- Covered Information retained by a non-Part 2 provider must be segregated from other patient records and retain the Notice regarding restriction on Non-Disclosure.
- Covered Information does not include information conveyed orally by a Part 2 Program to a non-Part 2 provider for treatment purposes with the consent of the patient even if reduced to writing by the non-Part 2 provider or information that is a summary created by the non-Part 2 provider of the information.
- Part 2 does not apply to information on Substance Use Disorder patients maintained in connection with the Department of Veterans Affairs' provision of hospital care, nursing home care, domiciliary care, and medical services under Title 38, U.S.C.

Covered Patient(s) means any Individual who has applied for or been given Diagnosis, Treatment, or referral for Treatment for a Substance Use Disorder at a Part 2 Program. The term Covered Patient includes any Individual who, after arrest on a criminal charge, is identified as an Individual with a Substance Use Disorder in order to determine that Individual's eligibility to participate in a Part 2 Program. This definition includes both current and former patients.

Covered Program means a program that is *Federally Assisted* and includes: (a) an Individual or entity (other than a general medical facility) who *holds itself out* as providing, and provides, Substance Use Disorder Diagnosis, Treatment, or referral for Treatment; (b) an *identified unit* within a general medical facility that holds itself out as providing, and provides, Substance Use Disorder Diagnosis, Treatment, or referral for Treatment (this includes a provider practice); or (c) medical personnel or other staff in a general medical facility whose *primary function* is the provision of Substance Use Disorder Diagnosis, Treatment, or referral for Treatment and who are identified as such specialized medical personnel or other staff within the general medical care facility.

- Covered Programs include, but are not limited to, those Treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, and private practitioners who hold themselves out as providing, and who provide Substance Use Disorder Diagnosis, Treatment, or referral for Treatment who are treated as receiving direct or indirect federal assistance through Medicare participation, tax-exemption or other criteria as set forth in 42 CFR § 2.12.
- Physicians who prescribe controlled substances to treat substance Use disorders are DEA-licensed and thus meet the test for federal assistance, but is not a Covered Program unless one of the other criteria are also met.
- An Individual or entity is considered to "hold itself out" when there is any activity that would lead one to reasonably conclude that the Individual or entity provides Substance Use Disorder diagnosis, treatment, or referral for treatment including but not limited to: (a) authorization by the state or federal government (e.g. licensed, certified, registered) to provide, and provides, such services, (b) advertisements, notices, or statements relative to such services, or (c) consultation activities relative to such services.

Diagnosis means any reference to an Individual's Substance Use Disorder or to a condition which is identified as having been caused by that Substance Use Disorder which is made for the purpose of Treatment or referral for Treatment.

Disclose or Disclosure means to communicate any information identifying a patient as being or having been diagnosed with a Substance Use Disorder, having or having had a Substance Use Disorder, or being or having been referred for Treatment of a Substance Use Disorder either directly, by reference to publicly available information, or through verification of such identification by another person.

Federally Assisted. A Covered Program is *federally assisted* if:

1. It is conducted in whole or in part, whether directly or by contract or otherwise by any department or agency of the United States (unless an exemption applies);
2. It is being carried out under a license, certification, registration, or other authorization granted by any department or agency of the United State including but not limited to:
    a. Participating provider in the Medicare program;
    b. Authorization to conduct maintenance treatment or withdrawal management; or
    c. Registration to dispense a substance under the Controlled Substance Act to the extent the controlled substance is used in the treatment of substance use disorders;
3. It is supported by funds provided by any department or agency of the United States by being:
    a. A recipient of federal financial assistance in any form, including financial assistance which does not directly pay for the substance use disorder diagnosis, treatment, or referral for treatment; or

b. Conducted by a state or local government unit which receives federal funds which could be spent for the substance ue disorder program; or

4. It is assisted by the Internal Revenue Service through the allowance of income tax deductions for contributions to the program or through the granting of tax exempt status to the program.

Maintenance Treatment means long-term pharmacotherapy for individuals with Substance Use Disorders that reduces the pathological pursuit of reward and/or relief and supports remission of Substance Use Disorder-related symptoms.

Member program means a withdrawal management or maintenance treatment program which reports patient identifying information to a central registry and which is in the same state as that central registry or is in a state that participates in data sharing with the central registry of the program in question.

Minor means a minor as defined by state law.

Patient Identifying Information means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a Covered Patient can be determined with reasonable accuracy either directly or by reference to other information. The term does not include a number assigned to a Covered Patient by a Covered Program, for internal Use only by the Covered Program, if that number does not consist of or contain numbers (such as a social security, or driver's license number) that could be Used to identify a Covered Patient with reasonable accuracy from sources external to the Covered Program.

Program Director means the Individual designated as the “Program Director” for the relevant Covered Program. For purposes of this Part 2 Policy, a Program Director may be the Chief Executive Officer of a free-standing behavioral health hospital, a Director of an inpatient behavioral health unit, or a Director or Manager of an outpatient behavioral health program.

Qualified Service Organization means an Individual or entity who: (a) provides services to a Covered Program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and Individual and group therapy, and (b) has entered into a written agreement with a Covered Program under which that Individual or entity: (i) acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the Covered Program, it is fully bound by the regulations in this part; and (ii) if necessary, will resist in judicial proceedings any efforts to obtain access to Patient Identifying Information; and (c) a Business Associate, as defined under the HIPAA Policy Manual, for a Part 2 Program that is also a Covered Entity, with respect to the Use and Disclosure of PHI that also constitutes Covered Information.

A business associate agreement that includes the terms referenced above through execution of a Quality Service Organization Addendum or other written agreement approved by the Privacy Officer may satisfy the requirements of subsection (b) above with respect to Qualified Service Organizations.

Audit/Evaluation Personnel means a person who: (a) performs an audit or evaluation on behalf of: (i) any federal, state, or local government agency which provides financial assistance (including, without limitation, Medicare reimbursement or other financial assistance) to the Covered Program or is authorized by law to regulate its activities; or (ii) any Individual or entity who provides financial assistance to the Covered

Program, which is a third party payer covering patients in the Covered Program, or which is a quality improvement organization performing a utilization or quality control review; or (b) is determined by the Program Director (in consultation with the Privacy Official) to be qualified to conduct the audit or evaluation.

Substance Use Disorder means a cluster of cognitive, behavioral, and physiological symptoms indicating that the Individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky Use, and pharmacological tolerance and withdrawal. For the purposes of this Part 2 Policy, Substance Use Disorder does not include tobacco or caffeine Use.

SUD Counseling Notes means notes recorded (in any medium) by a Part 2 Program provider who is a SUD or mental health professional documenting or analyzing the contents of conversation during a private SUD counseling session or a group, joint, or family SUD counseling session and that are separated from the rest of the Patient's SUD and medical record. SUD counseling notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Third-party Payer means an Individual or entity who pays and/or agrees to pay for Diagnosis or Treatment furnished to a patient on the basis of a contractual relationship with the patient or a member of the patient's family or on the basis of the patient's eligibility for federal, state, or local governmental benefits.

Treating Provider Relationship means that, regardless of whether there has been an actual in-person encounter: (a) a patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated, or agrees to accept consultation, for any condition by an Individual or entity, and; (b) the Individual or entity undertakes or agrees to undertake Diagnosis, evaluation, and/or Treatment of the patient, or consultation with the patient, for any condition.

Treatment means the care of a patient suffering from a Substance Use Disorder, a condition which is identified as having been caused by the Substance Use Disorder, or both, in order to reduce or eliminate the adverse effects upon the patient.

Undercover Agent means any federal, state, or local law enforcement agency or official who enrolls in or becomes an employee of a Part 2 Program for the purpose of investigating a suspected violation of law or who pursues that purpose after enrolling or becoming employed for other purposes.

Withdrawal Management means the Use of pharmacotherapies to treat or attenuate the problematic signs and symptoms arising when heavy and/or prolonged substance Use is reduced or discontinued.

POLICY:

1. **Identification of Covered Programs**. Provider shall identify and maintain an inventory of all Covered Programs and professionals diagnosing, treating or referring patients for treatment in a Covered Program and holding themselves out as such a specialized professional. The listing of Covered Programs will be updated periodically as there are changes.
    a. Provider will maintain an inventory of all non-Part 2 providers who have received and maintained Covered Information in the patient records.

2. **Identification and Segregation of Covered Information**. Provider shall assess and maintain an inventory of all locations of Covered Information.
    a. Once identified, the redisclosure notice shall be attached to each such Covered Information if not already placed on the document.
    b. Covered Information received by a non-Part 2 provider may be segregated to ensure that records of the non-Part 2 provider will not become subject to Part 2.

3. **Patient Access and Restrictions on Use**. Patients have a right to access and obtain a copy of their Part 2 records/Covered Information without requiring patient consent or authorization. Information disclosed to a patient is restricted from use to initiate or substantiate any criminal charges against the patient or to conduct any criminal investigation of the patients.

a. No Right to Access SUD Counseling Notes. Notwithstanding the foregoing, Patients do not have a right to access SUD Counseling Notes maintained separate from the rest of the Patient's record. As a general policy, Provider should not Disclose SUD Counseling Notes pursuant to any request, except if compelling circumstances exist for making such Disclosure as determined by the Privacy Officer. Provider must obtain a separate written consent to use or disclose a Covered Patient's SUD Counseling Notes. SUD Counseling Notes cannot be used or disclosed based on a broad consent for treatment, payment, and health care operations. For purposes of this Section, a "compelling circumstance" exists if non-disclosure would result in a barrier to patient care and such information is not available by other means. If a Disclosure is made under this Section, the Privacy Officer will document the compelling circumstances for making the Disclosure. The Privacy Officer may consult with legal counsel regarding Disclosures pursuant to this Section.

b. Disclosures pursuant to an appropriate Court Order: Provider may Disclose Covered Information subject to a subpoena if authorized by an appropriate order of a court of competent jurisdiction granted after application showing good cause.
    i. Covered Information by this Part 2 policy may not be Disclosed based upon a subpoena alone or a court order alone without a subpoena. Law enforcement must present both, a valid court order *and* subpoena.
    ii. Covered Information disclosed without consent for research purposes may not be compelled through a court order when the purpose of the request is for criminal investigation or prosecution of the patient.
    iii. A valid court order may authorize disclosure only if:
        - disclosure is necessary to protect against an existing threat to life or of serious bodily injury, including circumstances which constitute suspected child abuse and neglect and verbal threats against third parties; or
        - disclosure is necessary in connection with investigation or prosecution of an extremely serious crime, such as one which directly threatens loss of life or serious bodily injury, including homicide, rape, kidnapping, armed robbery, assault with a deadly weapon, or child abuse and neglect; or
            - The court order must: (1) limit use and disclosure to those SUD Records, or testimony essential to fulfill the objective of the order; (2) limit disclosure to those law enforcement and prosecutorial officials responsible for, or are conducting, the investigation or prosecution, and limit their use of the records or testimony to investigation and prosecution of the extremely serious crime or suspected crime specified in the application; and (3) include other measures as necessary to limit use and disclosure to the fulfillment of only that public interest and need found by the court.
        - disclosure is in connection with litigation or an administrative proceeding in which the patient offers testimony or other evidence pertaining to the content of the confidential communications.
            - The court order must (1) limit use or disclosure to only those parts of the patient's SUD Record, or testimony essential to

fulfill the objective of the order; (2) limit use or disclosure to those persons whose need for information is the basis for the order; and (3) includes measures necessary to limit use or disclosure for the protection of the Patient, the physician-patient relationship and the treatment services (e.g., sealing from public record).

- disclosure is to an investigative agency having jurisdiction over the Covered Program in order to investigate or prosecute the Covered Program in connection with a criminal or administrative matter, and the Covered Information is material evidence to its investigation or prosecution of the Covered Program.
    - The court order must (1) limit use or disclosure to only those parts of the patient's SUD Record, or testimony essential to fulfill the objective of the order; (2) limit use or disclosure to those persons whose need for information is the basis for the order; (3) includes measures necessary to limit use or disclosure for the protection of the Patient, the physician-patient relationship and the treatment services (e.g., sealing from public record); and (4) require redaction of patient identifying information from any documents or oral testimony made available to the public.
    - No information obtained hereunder may be used or disclosed to conduct any investigation or prosecution of a Patient in connection with a criminal matter, or be used or disclosed as the basis for an application for an order under criminally investigate or prosecute a Patient.

iv. If it is determined that the Provider requires an application for a Court Order, the Provider shall refer to the Privacy Officer to consult with legal counsel.

c. Disclosure to FDA in the Event of Potential Harm. Provider may Disclose Covered Information to medical personnel of the Food and Drug Administration (FDA) who assert a reason to believe that the health of any individual may be threatened by an error in the manufacture, labeling, or sale of a product under FDA jurisdiction, and that the information will be used for the exclusive purpose of notifying patients or their physicians of potential dangers. The Privacy Official shall be consulted prior to any Disclosure of information pursuant to this provision. Immediately following any Disclosure pursuant to this provision, the Provider shall document the Disclosure in the patient's records, setting forth in writing: (1) the name of the medical personnel to whom Disclosure was made and their affiliation with the FDA; (2) the name of the individual making the Disclosure; (3) the date and time of the Disclosure; and (4) The nature of the error.

d. Disclosure for Public Health. Provider may Disclose Covered Information for public health purposes without patient consent so long as: (i) the Disclosure is made to a Public Health Authority (as defined by HIPAA); and (ii) the Covered Information disclosed is de-identified such that there is no reasonable basis to believe that the Covered Information can be used to identify a Covered Patient.

4. **Consents Generally and TPO Consent**
    - **a.** Consent for Treatment, Payment, and Health Care Operations**.** Covered Patients may execute a single general written consent for all future uses and disclosures for Treatment, Payment and Health Care Operations of Provider ("TPO Consent"), except for uses and disclosures for civil, criminal, administrative, and legislative proceedings against Covered Patients. Electronic signature may be used. The TPO Consent will apply to all future uses and disclosures, including re-disclosures, made in accordance with HIPAA unless revoked by the Covered Patient. This consent may not be combined with a HIPAA Authorization and is distinct from a HIPAA Authorization.
    - **b.** Prior to making any re-disclosures, the Provider must ask the disclosing entity to confirm whether the Covered Patient has given written consent for all future uses and disclosures in accordance with HIPAA.

5. **Consent for Disclose to Family Members/Friends/Others Involved in Patient's Care**. The regulations under 42 CFR Part 2 do not include any exceptions specifically for Disclosures of Covered Information to family members, close friends or others identified by the Covered Patient. Accordingly, unless otherwise expressly permitted by this Part 2 policy or pursuant to an appropriate consent/authorization, Covered Information should not be Disclosed to family members, friends or others who might otherwise be considered involved in a patient's care.

6. **Responding to Requests**. In any case where Provider receives a request for Disclosure of Covered Information but where this Part 2 policy does not allow Disclosure, any response must be made in a way that will NOT affirmatively reveal that an identified individual has been, or is being, diagnosed or treated for a Substance Use Disorder. An inquiring party may be referred to 42 C.F.R. Part 2 and advised that the regulations restrict the Disclosure of Substance Use Disorder patient records, but may not be told affirmatively that the regulations restrict the Disclosure of the records of an identified Patient. Upon receipt of a request for Covered Information:

    a. If consent is required, has the patient consented to disclosure? If so, then the disclosure may be made but only as specifically provided in the valid consent.

    b. Each disclosure made with the Patient's written consent must be accompanied by a copy of the consent or a clear explanation of the scope of the consent provided. Each Disclosure made with the patient's written consent must be accompanied by one of the following written ***Notice Statements***:

        i. Statement 1. *This record which has been disclosed to you is protected by Federal confidentiality rules (42 CFR part 2). These rules prohibit you from using or disclosing this record, or testimony that describes the information contained in this record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against the patient, unless authorized by the consent of the patient, except as provided at 42 CFR 2.12(c)(5) or as authorized by a court in accordance with 42 CFR 2.64 or 2.65. In addition, the Federal rules prohibit you from making any other use or disclosure of this record unless at least one of the following applies: (i) Further use or disclosure is expressly permitted by*

the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2. (ii) You are a HIPAA covered entity or business associate and have received the record for treatment, payment, or health care operations, or (iii) You have received the record from a HIPAA covered entity or business associate as permitted by 45 CFR part 164, subparts A and E. A general authorization for the release of medical or other information is NOT sufficient to meet the required elements of written consent to further use or redisclose the record (see 42 CFR 2.31).

ii. Statement 2. *"42 CFR part 2 prohibits unauthorized use or disclosure of these records."*

c. If no consent has been provided and disclosure is not otherwise permitted under this Part 2 policy, provide the requestor with the Notice of Privacy Practices, this Part 2 policy, or a copy of the Part 2 regulations.

d. Where a subpoena is received *without a Court Order*, the recipient will, consistent with Provider policies, provide a timely written response by referring the relevant party to 42 C.F.R. Part 2, and providing any other records that may be lawfully provided without violation of 42 C.F.R. Part 2 and as permitted by HIPAA. As noted above, a party requesting information pursuant to a subpoena may be referred to 42 C.F.R. Part 2, but may not be told affirmatively that the regulations restrict the Disclosure of the records of an identified patient.

e. Where a subpoena has been received and a Court Order issued, response is required unless the subpoena has expired or there is another valid legal defense.

7. **Security Precautions**. Appropriate security will be maintained with respect to Covered Information, consistent with the security standards, policies and procedures of the Provider. Security measures will reasonably protect against unauthorized uses and Disclosures of Patient Identifying Information and protect against reasonably anticipated threats or hazards to the security of Patient Identifying Information. These formal policies and procedures address:
    a. Paper records, including:
        i. Transferring and removing such records;
        ii. Destroying such records, including sanitizing the hard copy media associated with the paper printouts, to render the Patient Identifying Information non-retrievable;
        iii. Maintaining such records in a secure room, locked file cabinet, safe, or other similar container, or storage facility when not in use;
        iv. Using and accessing workstations, secure rooms, locked file cabinets, safes, or other similar containers, and storage facilities that use or store such information; and
        v. Rendering Patient Identifying Information non-identifiable in a manner that creates a very low risk of re-identification (e.g., removing direct identifiers).
    b. Electronic records, including:
        i. Creating, receiving, maintaining, and transmitting such records;

ii. Destroying such records, including sanitizing the electronic media on which such records are stored, to render the Patient Identifying Information non-retrievable;

iii. Using and accessing electronic records or other electronic media containing Patient Identifying Information; and
iv. Rendering the Patient Identifying Information non-identifiable in a manner that creates a very low risk of re-identification (e.g., removing direct identifiers).

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

28. TRAINING ON HIPAA PRIVACY AND SECURITY POLICIES

28.1 POLICY STATEMENT

It is the policy of Provider to train all members of its workforce on the policies and procedures required by the HIPAA Privacy Rule and Security Rule with respect to PHI as necessary and appropriate for Workforce Members to carry out their functions.

28.2 SCOPE OF THIS POLICY

This policy applies to all Provider Workforce Members, including any employees whose job descriptions allow them to access individuals' PHI.

28.3 PURPOSE OF POLICY

To set forth the training all Workforce Members must receive regarding the policies and procedures required by the Privacy Rule and Security Rule.

28.4 POLICY DETAIL

Provider has provided or will provide training as follows:

- To each member of Provider's workforce by no later than the date by which Provider begins using and disclosing PHI.
- Thereafter, to each new member of the workforce during new hire orientation and within a reasonable period of time after the person joins Provider's Workforce.
- To each member of Provider's workforce whose functions are affected by a material change in Provider's policies or procedures within a reasonable period of time after the material change becomes effective.

CONTENT OF TRAINING. Training sessions may include the following:

- Awareness training (live lecturing or video-based training).
- How to identify phishing attacks and ransomware attacks and how to respond to these types of incidents; as well as avoiding misdirected emails.
- Prohibited practices including taking unauthorized photographs and recordings of patients.
- Details of applicable policies and procedures.
- Periodic security reminders (via the Use of methods such as e-mails, bulletin boards, pamphlets, staff meetings, etc.).
- Timely information about changes in policies and procedures.
- Information about sanctions.

DOCUMENTATION. Provider will document that the training has been provided by:

- maintaining the policies and procedures in written or electronic form;

- maintaining a record of the attendance of each Workforce Member at any required training session on the Privacy Rule, these privacy policies or general training on maintaining the privacy and confidentiality of PHI;
- maintaining a record of any voluntary training undertaken by any Workforce Member on the Privacy Rule, these privacy policies or general training on maintaining the privacy and confidentiality of PHI;
- maintaining a record of the test results of any Workforce Member following any required or voluntary training session where testing of the material presented occurred; and
- ensuring that for any action, activity, or documentation regarding training that is required by the Privacy Rule or Security Rule to be documented, a written or electronic record of such action, activity or documentation is maintained.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

29. DISCIPLINARY SANCTIONS FOR NONCOMPLIANCE WITH PROVIDER'S PRIVACY AND SECURITY POLICIES

29.1 PURPOSE OF POLICY

To set forth the appropriate disciplinary procedures for Workforce Members who fail to comply with these privacy policies and procedures and to ensure compliance with the Privacy Rule and Security Rule.

29.2 POLICY DETAIL

Provider will apply the same progressive disciplinary procedures to Workforce Members who fail to comply with these policies and procedures, up to and including termination for serious and/or repetitive violations, as it applies to all other instances of employee misconduct.

In the opinion of the Privacy Official and/or the Security Official, should the violations of a Workforce Member be deemed to be "serious," or the repetition of the violation be deemed evidence of a willful disregard of these policies, the Privacy Official and/or the Security Official may impose an appropriate sanction without regard to progressive levels of discipline.

This policy does not apply to Workforce Members with respect to actions that are: (1) covered by and that meet the conditions of Disclosures by whistleblowers, (2) Disclosures by Workforce Member(s) who are crime victims, or (3) for those employees exercising any right under the Privacy Rule.

Provider will document the sanctions that are applied, if any, and retain such documentation for six years from the date of its creation or the date when it was last in effect, whichever is later.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

30. REPORTING AND MITIGATING INADVERTENT OR IMPROPER DISCLOSURES OF PHI OR SECURITY INCIDENTS

30.1 PURPOSE OF POLICY

To ensure that the consequences of any impermissible or inadvertent Disclosure of Individual PHI or Security Incidents are minimized to the extent possible and to comply with the requirements of the Privacy and Security Rule.

30.2 POLICY DETAIL

Workforce Members who are aware of or who become aware of an impermissible or inadvertent Disclosure of Individual PHI should report the occurrence to the Privacy Official.

Workforce Members who are aware of or who become aware of a Security Incident related to or involving Individual PHI should report the occurrence to the Security Official.

Upon receipt of such a report, the Privacy Official or Security Official will investigate the reported incident to determine the nature of the Disclosure, to whom the Disclosure was made, the circumstances under which it was made, and the reasons why it was made (to the extent possible).

The Privacy Official, Security Official, or his or her designee, will respond in a manner that will mitigate or minimize the consequences of the incident to the extent possible. This may include but is not limited to:

- contacting persons or entities to which the Disclosure was made to determine what further Uses or Disclosures of the PHI may have occurred;
- whenever possible, seeking to stop any further Uses and/or Disclosures of the PHI;
- correcting, where appropriate, any wrong or inaccurate information that was involved in the Disclosure;
- whenever possible, seeking the return of all information improperly Disclosed;
- if the situation rose to the level of a Breach, review the Breach and revise the information security program and the Provider's business practices to minimize the likelihood of a recurrence of the same, or a similar Breach;
- sanctioning any Workforce Member(s) responsible for the Disclosure;
- addressing the matter with any Business Associate responsible for the Disclosure and requiring the Business Associate to cure any inadequacies in its physical, technical or administrative systems that contributed to the Disclosure or terminating Provider’s agreement with the Business Associate should the Business Associate fail to cure the defect in a reasonable period of time or should the failure not be subject to cure; and
- reporting the Disclosure to the Provider’s legal counsel if, in his or her view, the Disclosure is of a nature that could give rise to litigation.
- documenting each incident involving a Breach of the privacy or security measures implemented by the Provider to protect PHI (each an "Incident Report"). Each Incident Report will include, at a minimum: (i) a post-incident review of the Breach itself, (ii) the responsive actions taken in connection with the

Breach, and (iii) those revisions to the Information Security Program or the Provider's business practices that were made to minimize the likelihood of a recurrence of the same, or a similar Breach.

The initial and primary focus of all activities undertaken by the Privacy Official, the Security Official or any Workforce Member in response to a Disclosure of PHI in violation of HIPAA, or these policies will be to mitigate, to the extent practicable, any harmful effects of the violation that become known or which reasonably should become known through the exercise of reasonable diligence.

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

31. ADMINISTRATIVE, TECHNICAL AND PHYSICAL PRIVACY AND SECURITY SAFEGUARDS

31.1 PURPOSE OF POLICY

To ensure that Individual PHI is not intentionally or unintentionally Used or Disclosed in violation of the Privacy Rule or Security Rule.

31.2 POLICY DETAIL

Recognized Security Practices. [If the organization has adopted "recognized security practices," defined as the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities," document here how "recognized security practices" are implemented, including implementation of any specific elements or sub-practices of the "recognized security practices" and the scope of implementation throughout the organization the names of individuals responsible for ensuring "recognized security practices" are implemented by workforce members; training materials provided to workforce members on "recognized security practices" and dates of training, and documentation showing whether "recognized security practices" were developed under: (i) Section 2(c)(15) of the National Institutes of Standards and Technology Act; (ii) the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; and (iii) other programs and processes that address cybersecurity that are developed, recognized or promulgated through regulations under other statutory authorities (include regulatory or statutory citations)."]

RISK ANALYSIS, EVALUATION OF SECURITY, AND ONGOING RISK MANAGEMENT. The risk analysis is a process that may be used to identify possible threats and vulnerabilities, and to identify possible ways to reduce risk. The Security Official shall work with the Privacy Official, legal counsel, and other operational and business representatives (the "RM Group") to conduct an initial, comprehensive risk analysis of the safeguards in place to protect ePHI. The Security Official may also utilize HHS risk

assessment tools.[1]The initial risk analysis will create a baseline for ongoing and future risk management and evaluation activities. The RM Group will determine how identified risks will be managed so that vulnerabilities will be brought to a reasonable and appropriate level. The RM Group will document how risks will be mitigated and managed.

The Security Official, with the assistance of the RM Group, as needed, will periodically (whenever environmental or operational changes affecting PHI occur) review and evaluate the risks to the security of PHI and these HIPAA policies to determine whether changes are needed for ongoing compliance. Risks will be evaluated based on the impact of the risk and the probability of occurrence. Risks must be documented, along with a plan to mitigate the risks.

The Risk Analysis must contain:

- A defined scope that identifies all of its systems that create, transmit, or maintain ePHI
- Details of identified threats and vulnerabilities
- Assessment of current security measures
- Assessment of the impact of the risk and the likelihood of such risk occurring
- Risk rating.

The RM Group will be responsible for documenting and performing ongoing risk management functions as needed, including periodic review and evaluation of technical solutions, policies and procedures, workforce training, employee compliance with existing policies and procedures, business associate agreements, and effectiveness of audits, including the means implemented for detecting and preventing failures of the security measures put in place to protect PHI. The RM Group will determine what measures to take to address any particular risk. Depending on Provider's size, complexity, capabilities, technical infrastructure, and the probability and criticality of potential risks to Provider's PHI, the RM Group may choose to do nothing if the level of risk is acceptable; reduce or mitigate the risk; or transfer the risk to another organization by contracting with a vendor to help manage the risk. To the extent Workforce Members or their duties are substantially affected by a chosen action, the Privacy Official and Security Official shall be responsible to provide appropriate training.

ACTIVITY REVIEW OF EPHI SYSTEM SECURITY. Appropriate Information Technology personnel assigned as Workforce Members for Provider or an appropriate Business Associate providing IT services to Provider ("IT Group") shall audit the access privileges for each Workforce Member at least once every twenty-four (24) months. The IT group must periodically run reports to review system activity, such as audit logs, access reports, or security incident tracking reports, to determine whether external unauthorized Users are trying to penetrate Provider's systems and servers. The reports should also consider the risks of any website pixels or other website tracking tools Used by the Provider or third parties. These reports will be run **[***insert frequency – every ___, hours/daily/ etc*.**]** using **[***insert current software name***]** or a similar appropriate software or product that tracks and reports suspected intrusions.

The IT Group must guard Provider's systems against malicious software and viruses using an appropriate anti-virus infrastructure such as **[***insert current software or system name and describe how it will be kept current. Also describe any other policies that may exist regarding sharing files between office and home computers, and downloading games, data, or other software. Discuss the hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or Use ePHI.***]**

[1] See www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

. Any suspicious activities must be reported to the Security Official. Any reports documenting such suspicious activities shall be maintained or archived in electronic or hard copy format and shall be accessible to the Security Official.

31.2.3 SAFEGUARDS.

Provider shall maintain four general categories of safeguards of PHI:

1. **Administrative Safeguards:** documented, formal policies and procedures that are intended to manage the selection and execution of security measures Used to protect data based upon the appropriate data classification standards and manage the conduct of personnel with respect to the protection of the data.

2. **Physical Safeguards:** protection of physical computer systems and the buildings holding such systems from natural and environment hazards and inappropriate intrusion or removal.

3. **Technical Safeguards:** processes put in place to protect information, authenticate Users and control Individual access to information.

4. **Organizational requirements:** provides requirements for the content of Business Associate contracts or other arrangements. The Policies and Procedures and Documentation Requirements section, among other things, requires covered entities to implement and maintain written policies, procedures and documentation required to comply with the Security Rule.

Safeguards to Protect PHI. Workforce members will be trained to protect PHI using various methods including the following:

- Workforce Members Accessing PHI on Covered Entity or vendor systems using only technology approved by the Privacy Official or Security Official.
- Physically securing hard copies or unencrypted PHI when not in Use (e.g. in a locked drawer)
- Refraining from filming or photographing PHI, or recording audio PHI in the workplace.
- Ensuring a clear workspace and properly securing PHI prior to leaving for a break or for the day.
- To the extent practicable, during emergency mode operations, safeguarding PHI in a manner similar to how it is safeguarded during normal operations.
- Refrain from removing PHI and portable devices containing PHI from the BA to the Covered Entity premises without prior approval from the owner/custodian. To the extent practicable, the data owner/custodian should maintain a log with a record of the date, information involved, and the person possessing the information.
- Refraining from storing PHI on the hard drive of a laptop unless authorized.
- Refraining from storing PHI on the hard drive of a personal computer.
- Refraining from storing PHI on a portable storage device (thumb drive, phone, disc, etc.) without approval from the Privacy Official or Security Official.
- Using password-protected screen savers and screen savers that are enabled when the computer is unattended for a significant amount of time.
- Logging off computers overnight or when unattended for a long period of time.

- Adequately concealing PHI from Disclosure to nearby unauthorized parties.
- Speaking in a reasonable tone of voice to minimize the chance that unauthorized persons will overhear discussions involving PHI.
- Refraining from transmitting or receiving PHI to or on the Workforce Member's personal email account.
- Refraining from sending PHI to unauthorized persons, or sending or using more PHI than necessary to do the job.
- Disposing of unneeded PHI property and in a secure manner such as shredding paper records, or completely wiping electronic PHI. Workforce Members must not destroy or dispose of Covered Entity-provided PHI unless authorized by the Privacy and Security Official.
- Refraining from printing PHI unless there is a business requirement.
- Refraining from installing unauthorized software.
- Ensuring the most current versions of firewalls and anti-virus software are installed on personal computers and mobile devices.

Termination or Modification of Access to PHI: Electronic Systems. Provider must implement policies and procedures that establish access to ePHI and to modify or terminate that access as needed.

Access Controls. Provider must implement facility and device access controls to protect devices that hold PHI through the Use of keys, locks, visitor escorts, fire protection, and access profiles that describe who may access such devices. Device and media controls are intended to assure that ePHI, as well as the device where it is stored, is destroyed in a manner that ensures that the ePHI cannot be re-created. Authentication and validation controls are Used to corroborate that a person is the one claimed or the data has not been altered or destroyed in an unauthorized manner.

Access Restrictions for Physical and Electronic Records. Physical access restrictions to paper-based records and media containing PHI and ePHI shall be implemented. Such restrictions include, for example, limiting access by securing applicable paper-based records in locked facilities or containers, limiting the number of available keys to locked facilities or containers, and only allowing supervised access to the relevant records.

Secure Storage of Physical Records. Relevant records in paper-based form will be stored in locked facilities, storage areas or containers. In addition, the Security Official shall take steps to ensure that relevant facilities, storage areas and containers are locked at the end of the working day, and that employees using relevant records in paper-based form return these records to their storage locations before leaving work for the day.

Access Restrictions for Electronic Records. Access to electronic versions of records containing PHI shall be restricted to only those Workforce Members who need access to such records to perform their daily job responsibilities. Such restrictions may include, for example, isolating electronic records to a storage location that is only accessible by employees with appropriate administrative privileges.

Identification and Passwords. Unique User accounts and passwords shall be assigned to all employees with computer access. Such assignments shall be reasonably designed to maintain the integrity and security of all implemented access controls. Assigned passwords shall not be vendor-supplied default passwords. User passwords shall be reset at pre-determined intervals and prohibitions against selecting

previously-Used passwords shall be implemented. The Security Official or his or her designee is responsible for password management, including password length and configuration, limiting the number of log-in attempts, monitoring expiration and discrepancies, deactivation, automatic logout, and automatic updates.

Secure User Authentication Protocols. The following additional security measures shall be implemented:

- Maintaining controls on User IDs and other identifiers;
- Enforcing secure methods of assigning and selecting passwords;
- Maintaining controls for data security passwords that ensure that such passwords are kept in a location and/or format that does not compromise the security of the records they protect;
- Requiring re-login of a User should a computer remain inactive for an extended period of time; and
- Restricting access to records containing ePHI to only active Users and active User accounts.

Firewall Protection. Firewall protection shall be installed on all computers in Covered Entity's control that store or are able to access records containing ePHI. The Security Official will also take reasonable steps to ensure that the installed firewall protection is up-to-date, and will regularly update firewall protections as newer versions and patches become available.

Virus Protection. The Security Official will take reasonable steps to ensure that the Covered Entity's network contains: (i) malware protection, (ii) reasonably up-to-date patches; and (iii) reasonably up-to-date virus definitions, for purposes of protecting records containing ePHI.

Encryption of PHI. The term "**encrypt**" or "**encryption**" means the transformation of data into a form in which meaning cannot be assigned without the Use of a confidential process or key.

Encryption of Stored PHI. Unless a documented analysis determines that encryption is not reasonable and appropriate, the Security Official will encrypt all PHI stored on laptops or other portable or mobile devices in Covered Entity's control that are capable of storing, receiving or transmitting records containing ePHI.

Encryption of PHI During Transmission. The Security Official will, to the extent technically feasible, introduce encryption processes for records containing ePHI that are transmitted by electronic means over public networks (whether wireless or wire-line).

Workstation Use and Location. Provider will provide secure workstations and computer terminals with physical safeguards and technical access controls to minimize the possibility of unauthorized Use or Disclosure of PHI. Computer screens at each workstation will be in secure areas or set up in a manner that permits only authorized Users to read any PHI that could be on the screen. If screens cannot be positioned to prevent unauthorized viewing, the Provider may Use devices, such as filters or hoods, to protect the screen from unauthorized viewing. Computer screens will be configured to display a screen saver or go blank and log off when left unattended for a certain period of time as determined by the Security Official. A password will be required to re-activate the screen. When applicable, paper documents that contain PHI must not be placed in a location where the PHI can be seen by unauthorized persons. For example, papers containing PHI should not be left face up on a counter unattended.

System Usage. Provider will monitor system usage by limiting the number of log in attempts to __, and require that systems automatically log out after __minutes of inactivity even when used by an authorized user.

Facsimile Machines and PHI. PHI may be sent via facsimile machine ("fax"), as long as the Provider takes reasonable precautions to protect the data. Such precautions may include measures such as:

- Including a confidentiality statement on the fax cover sheet indicating that the information is legally protected and, if the fax is received in error, the recipient should not re-Disclose the information and should contact the sender immediately to arrange for the documents to be destroyed or returned.
- The sender should Use caution to confirm that the number has been programmed correctly into the machine.
- If the machine has memory and storage capabilities, Provider must ensure that PHI is properly wiped from the machine when returning or discarding the machine.
- Provider should take reasonable precautions to ensure that faxes will be expected by the recipient and received by the recipient in a secure manner.

- **E-mail and PHI**. All e-mail correspondence containing PHI should be encrypted when encryption is reasonable and appropriate. Provider should take steps to minimize the amount of PHI included in e-mail. The sender must take reasonable precautions to reduce the chance of a misdirected e-mail. For example, the sender should confirm that the address of the recipient is accurate before using it to send PHI. Texting methods, unless they are secure (such as through encryption), may not be Used to transmit ePHI. Workforce Members should Use the "reply to all" feature as infrequently as possible. When sending emails containing PHI for an authorized purpose outside the organization, the email should be encrypted. The Security Official will assess the effectiveness of Provider's ability to balance the confidentiality of the PHI with its integrity and availability.

Copy Machines. The Security Official will review any storage capability of copy machines and determine whether they store ePHI that must be secured, particularly before copy machines are sold or discarded.

General Guidelines to Safeguard PHI. During business hours, a Workforce Member must be present whenever people who are not authorized to access PHI in that particular area are in the area where PHI is stored. After hours, if PHI will be unattended, it should be in a locked area. PHI in hard copy no longer in Use must be shredded, burned, or otherwise rendered unusable, unreadable, or indecipherable, in accordance with federal guidance, when the Provider no longer needs to retain it. PHI held for a shredding service, must be kept in a locked container or a container that is not accessible by unauthorized personnel.

Transmission Security. Provider must ensure information is only transmitted to the intended Individual or entity, and that there are measures in place to guard against unauthorized access to ePHI transmitted over a communications network.

Integrity.

[*Address mechanisms to ensure integrity of data during transmission – including portable media transmission (laptops, cell phones, thumb drives).* Document policies and procedures to protect ePHI from

improper alteration or destruction. Document policies and procedures to ensure that electronically transmitted ePHI cannot be improperly modified without detection until disposed of properly.]

Contingency Planning and Data Backup. Provider should refer to its *Disaster Recovery Plan* to restore any significant loss of data and to allow the continuation of the protection of ePHI while operating in a disaster situation or emergency mode. Provider, through its Business Associates and the IT Group, will implement a mechanism to protect ePHI from improper Use and Disclosure while minimizing the total impact on business operations in response to a crisis. The IT Group is responsible for restoring any loss of ePHI due to an emergency, power loss, natural disaster, vandalism, fire, movement or replacement of equipment or other occurrences and assisting Workforce Members with emergency mode operations. The Security Official shall work with the IT Group to assess the relative criticality of specific applications that contain ePHI to assure the appropriate level of security and planning to minimize problems for critical business functions. The IT Group shall perform periodic tests or trials of disaster recovery plans and emergency mode operations. The IT Group will back up and retain data for as long as the Security Official deems necessary to protect the availability, integrity, and confidentiality of ePHI. After the expiration of the applicable retention period, backup tapes will be overwritten or degaussed by the IT Group. Backup tapes will be retained for __ years.

Audit Trails. [*Indicate how records will be maintained when electronic data is accessed or changed.*]

DEPARTMENT:		**POLICY TITLE:**	
EFFECTIVE DATE:		**APPROVAL DATE:**	
APPROVED BY:		**POLICY NO.:**	
Regulations:			

32. VERIFICATION OF PERSONS REQUESTING PHI

32.2 PURPOSE OF POLICY

To ensure that Workforce Members, before disclosing PHI, have made reasonable efforts to ascertain or authenticate the identity of the persons or entities requesting a Disclosure of PHI so as to avoid violating the Privacy Rule and to minimize the likelihood of disclosing Individual PHI to people who are not entitled to that information.

32.3 POLICY DETAILS

Workforce Members must take steps to verify the identity of individuals who request access to Individual PHI. They must verify the authority of any person seeking access to Individual PHI, if the identity or authority of such person is not known to them.

Persons who are permitted access to a patient's Designated Record Set must be provided with electronic access to electronic records when requested, unless an information blocking exception applies (as provided under the 21st Century CURES Act).

REQUESTS MADE BY AN INDIVIDUAL. When an Individual requests access to his or her own PHI, Workforce Members will follow the steps below:

In Person Requests. Unless the Individual is personally known to the Workforce Member, Provider will request a form of identification from the Individual when the Individual requests an Individual's PHI in person. Workforce Members may rely on a valid driver's license or passport or other photo identification issued by a government agency. If the Individual does not have photo identification, the Workforce Member should request information that would be requested in connection with a telephone request, as set forth below. If a Workforce Member has any doubts as to the validity or authenticity of the identification provided or the identity of the Individual requesting access to the Individual's PHI, that person should contact the Privacy Official.

Telephone Requests. If the Individual requests PHI over the phone, the Workforce Member should request information that can be matched with information in the Individual's Designated Record Set, such as the last four numbers of his or her Social Security number or some other unique piece of information that can be Used to verify the caller's identity.

Electronic Access. When a request is for an electronic copy of a record that is also maintained electronically (such as in the EMR or online patient portal), the Patient may not be required to submit the request in writing prior to being provided access and unless an information blocking exception applies pursuant to the 21st Century Cures Act, the Patient must be given access to the electronic information as soon as possible. Access may not be delayed through any unreasonable efforts to verify identity.

REQUESTS BY PARENT SEEKING PHI OF A MINOR CHILD. When a parent requests access to PHI of the parent's minor child, Workforce Members will follow the steps below:

- Seek verification of the identity of the Individual through the steps described above.
- Seek verification of the person's relationship with the child. Such verification may take the form of confirming listing the child as a dependent in the Provider's records.
- Under laws of many States, a minor or unemancipated child may seek and agree to medical treatment in certain circumstances (*e.g.*, pregnancy or substance abuse) without parental involvement. In such instances, Provider may not be at liberty to Disclose the child's PHI to the parent.

To the extent not pre-empted by HIPAA or Part 2, Provider will comply with state law requirements applicable requests for access to PHI of a minor child by a parent. Workforce Members responsible for responding to requests for PHI should contact the Privacy Officer with any questions the Workforce Member may have regarding parental access to a minor patient's PHI.

REQUEST BY A PERSONAL REPRESENTATIVE. When a personal representative requests access to an Individual's PHI, Workforce Members will follow the steps below:

- The Workforce Member should require a copy of a valid power of attorney, or other appropriate document, that describes the basis for and authority of the Individual to act as the Individual's personal representative. If there are any questions about the validity of the document, the Workforce Member should seek review by the Privacy Official.
- The Workforce Member should make a copy of the documentation provided and file it with the Individual's Designated Record Set.
- The Disclosure should be documented according to Provider's documentation procedures.

REQUESTS BY A PUBLIC OFFICIAL. If a public official requests access to PHI and the request is for one of the purposes permitted under the Privacy Rule, Workforce Members will follow the steps below:

- If the public official is making the request in person, the Workforce Member should ask the public official to show an agency badge, ID or other official credential, or other proof of their status as a representative of the requesting agency. The Workforce Member should make a copy of the identification provided and file it with the Individual's Designated Record Set.
- If the request is made in writing, verify that the request is on the appropriate governmental agency letterhead.
- If the request is made by a person purporting to act on behalf of a public official, request a written statement on appropriate governmental agency letterhead that the person is acting under governmental authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding or purchase order that establishes that the person is properly acting on behalf of the public official.
- Request a written statement of the legal authority under which the information is requested or, if a written statement would be impracticable, an oral statement of such legal authority. If the official's

request is made pursuant to legal process, warrant, subpoena, order or other legal instrument issued by a grand jury, or a judicial or administrative tribunal, the Workforce Member should contact the Privacy Official.

- The Workforce Member should obtain approval for the requested Disclosure from the Privacy Official.
- The Disclosure should be documented according to Provider's documentation procedures.

Notwithstanding, if Provider is a Part 2 Program, then responding to requests by a public official or Law Enforcement Official must comply with 42 C.F.R. Part 2 and the *Part 2 Policy* to this *HIPAA Policy Manual*.