The Wright Center for Community Health ("TWCCH")

HIPAA Compliance Binder

Revised: March 2025

THE WRIGHT CENTER MEDICAL GROUP, P.C.

HIPAA COMPLIANCE BINDER

TABLE OF CONTENTS

	TAB
Confidentiality of Medical/Health Information Policies & Procedures	1
Authority/Identity Verification Form	2
Minimum Necessary Disclosure Log Form	3
Notice of Privacy Practices Acknowledgement of Receipt of Notice	4
Request of Restrictions Form	5
Request for Confidential Communications Form	6
Request for Access Form	7
Denial of Access From	7
Request for Amendment Form	8
Denial of Amendment Form	8
Request for Accounting Form	9
General Authorization Form	10
Business Associate Addendum	11
Notification to Individuals of Unsecured Protected Health Information Breach Notification to Media Outlets of Unsecured Protected Health Information Breach	12
Employee Confidentiality Statement	13

TAB 1

Policy Title: **HIPAA Policy**	
Policy Type: Administrative	*Policy Number:* 01.12.0001.P
Policy Owners: VP & Chief Compliance Officer	*Policy Approver:* SVP of Enterprise Integrity, Chief Legal and Governance Officer
Committee/Board Approval(s):	*Date Policy Originally Established:* August 30, 2019 Revised: April 24, 2020 Reviewed: September 18, 2024
Date(s) of Last Approval:	*Next Review Date:* September 18, 2025

PURPOSE

The Wright Center for Community Health (TWCCH) upholds safety as a primary value and is committed to nonviolence, emotional intelligence, open communication, democracy, social responsibility, social learning, and growth and change. A key component of living these committees and the value of safety is ensuring that the rights of individuals are protected and disclosed according to the federal and state rules and regulations.The purpose of the policies and procedures promulgated in this document is to protect individuals and the Provider from unlawful dissemination of information regarding the provision of and payment for treatment of patients, and specifically to comply with all federal and Commonwealth of Pennsylvania laws governing the protection of confidential medical information, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and all regulations developed by the Department of Health and Human Services ("HHS").This document provides specific guidelines for how the Provider will use and disclose "protected health information," or "PHI," (as defined in Section II herein) outlines the rights and obligations of the Provider and individuals in handling PHI, and provides forms, where needed, for documenting the use and disclosure of PHI. These policies apply equally to PHI in paper as well as electronic format. TWC utilizes the Entrepreneurial Operating System (EOS) to clarify, simplify and achieve its mission and vision. One of the six key components of the EOS model is Process which embodies the concept of developing policies and procedures that are clearly documented and are required to be followed by all.

SCOPE

This policy applies to all employees, contracted employees, and learners.

DEFINITIONS

1. PHI, for the purposes of the policies and procedures promulgated herein, shall mean any information relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, where such information either identifies the individual or where there is a reasonable basis to believe that the information could be used to identify the individual.
2. All employees providing healthcare and related services for or on behalf of Provider's patients, also known as "authorized personnel."
3. "Treatment" means the provision, coordination, or management of healthcare and related services by one or more health care providers.
4. "Payment" means activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and the provision of benefits, as well as activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.
5. "Health Care Operations" means certain operational and administrative tasks undertaken by a health care provider or health plan, including such things as
    a. quality assessment and quality improvement;
    b. reviewing and evaluating the competence or qualifications of health care professionals;
    c. contract placement, including underwriting, premium rating and other activities relating to the creation, renewal or replacement of a health insurance or health benefits contract;
    d. arranging for certain professional services such as legal or audit review services;
    e. business planning and development;
    f. resolution or internal grievances; and
    g. customer service activities.
6. Any ambiguities that arise with regard to whether certain activities fit into the definitions in this Section shall be resolved by contacting legal counsel.

POLICY

I. Policy Statement

It shall be the policy and purpose of The Wright Center for Community Health ("TWCCH") (the "Provider") to treat all information regarding the health care of individuals as confidential information, recognizing that such information is the property of such individuals, and that Provider receives this information solely and to serve its purposes as a provider of health care services.

II. Policy Purpose

The purpose of the policies and procedures promulgated in this document is to protect individuals and the Provider from unlawful dissemination of information regarding the provision of and payment for treatment of patients, and specifically to comply with all federal and Commonwealth of Pennsylvania laws governing the protection of confidential medical information, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and all regulations developed by the Department of Health and Human Services ("HHS").This document provides specific guidelines for how the Provider will use and disclose "protected health information," or "PHI," (as defined in Section II herein) outlines the rights and obligations of the Provider and individuals in handling PHI, and provides forms, where needed, for documenting the use and disclosure of PHI. These policies apply equally to PHI in paper as well as electronic format.

However, PHI relating to (i) substance abuse records, (ii) HIV/AIDS-related information, and (iii) psychotherapy notes is treated differently from other types of PHI, and will in all instances be disclosed to third parties only pursuant to a signed authorization, unless the disclosure is for treatment purposes, or related to the payment for treatment services.

III. Protection of PHI

A. Only the following representatives of the Provider are entitled to have access to PHI:
    1. All employees providing healthcare and related services for or on behalf of Provider's patients, also known as "authorized personnel."

B. PHI shall only be used or disclosed by such individuals in accordance with these policies and procedures. Specifically, but without in any way limiting the applicability of Section IV(B) below, Authorized Personnel shall use or disclose PHI as necessary to provide treatment services to individuals who visit WCMG for services, as well as to coordinate treatment efforts. In addition, Authorized Personnel may use and disclose PHI as needed to conduct "payment" (as that word is defined below) and to perform certain "health care operations" (as that term is defined below) necessary for the proper functioning of WCMG.

C. Authorized Personnel shall not share PHI with other employees or with third-parties who are not authorized in writing to access PHI. PHI shall only be used within the confined office space of WCMG, and shall not be left lying in areas where unauthorized persons may view or otherwise access it. When PHI is not in use, it shall be kept in locked filing cabinets that are not accessible by the general public.

D. Authorized Personnel shall sign a confidentiality agreement providing that he/she will take all reasonable efforts to protect the confidentiality of PHI.

E. In no event shall Provider or any of its Authorized Personnel sell PHI in exchange for any form of remuneration of any kind.

IV. Uses and Disclosures for which No Authorization Required.

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

B. Policy. It is policy of the Provider to use and disclose an individual's PHI for the purposes of conducting TPO, without first obtaining the individual's authorization, in the following circumstances:
    a) for the purposes of the Provider's TPO;
    b) for the treatment activities of any health care provider;
    c) for the payment activities of another health care provider or a health plan, as long as the recipient of PHI is that provider or health plan; or
    d) for the purposes of assisting another health care provider or a health plan with (i) fraud and abuse detection or compliance, or (ii) quality assessment and improvement activities relating to improving health or reducing health care costs; provided that Provider and the recipient entity both have a relationship with the individual who is the subject of the PHI.

C. Other Uses & Disclosures Not Requiring Authorization.
    1. Policy. The Provider is permitted by law to disclose PHI, without first obtaining an individual's written authorization, for the following purposes:
        a) public health purposes;
        b) health oversight activities;
        c) judicial and administrative proceedings;
        d) law enforcement;
        e) disclosures to personal representatives;

f) disclosures to family members involved in an individual's care;
g) to avoid serious threats to health and safety;
h) for workers' compensation functions;
i) to protect victims of abuse, neglect or domestic violence; and
j) to affect certain other government functions.

2. Limitation. Each of the above disclosures is subject to a number of legally mandated conditions, limitations and exceptions. All questions relating to the appropriate use and disclosure of PHI for the above purposes shall be resolved by contacting the HIPAA Compliance Officer.

V. Policy for Verification of Individuals or Entities Requesting Access to PHI.

The Provider shall take all steps necessary to verify and document the identity and legal authority of persons and entities requesting access to an individual's PHI. Such verification may include checking forms of identification, such as driver's license, birth certificate, agency badge (if the requestor represents a government entity), letterhead, or other forms of verifying the veracity of the requestor's identity and authority to access PHI. Verification of the requestor's identity and authority will be documented on the Authority/Identity Verification form.

VI. Minimum Necessary Policy

A. Policy

1. For third party disclosures that do not require the execution of an authorization, the Provider will follow proper procedures to ensure that only the minimum amount of PHI necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.
2. Authorized Personnel shall utilize only the minimum amount of PHI necessary to accomplish the specific purposes for which they are using the PHI.
3. This Minimum Necessary policy does not apply to the following uses or disclosures of PHI:
   a) disclosures to or requests by a health care provider for treatment;
   b) uses or disclosures made to the individual who is the subject of the PHI;
   c) uses or disclosures made pursuant to a valid authorization;
   d) disclosures made to the Department of Health and Human Services;
   e) uses or disclosures required by law; and
   f) uses or disclosures required in order for the Provider to comply with applicable laws and regulations

VII. Individual Rights

A. Policy on Notice of Privacy Practices

1. The Provider will provide a formal notice to individuals describing the ways in which the Provider uses and discloses protected health information, and all rights that individuals have with regard to their protected health information maintained by the Provider.
2. The Provider shall attempt, in good faith, to obtain written acknowledgment that the individual has received the notice at the earliest possible opportunity. Specifically, Provider shall furnish the notice to individuals with whom Provider has a direct treatment relationship as follows:
   a) no later than the date of the first service delivery;

b) upon request; and
c) on or after the effective date of a revision to the notice.

3. Except in an emergency treatment situation, the Provider will attempt to obtain acknowledgment of an individual patient's receipt of the notice on the first date of service following the implementation of these policies and procedures. Provider will ask the patient to sign an "Acknowledgement of Receipt of Notice" form, verifying that he or she has received the notice. If the individual refuses to sign this form, the Provider will document our efforts to obtain written acknowledgment and the reasons why the acknowledgment was not obtained.
4. In the event of an emergency treatment situation, Provider will furnish the individual with the notice as soon as reasonably practicable, and will attempt to obtain written acknowledgment of receipt at that time.
5. The Provider will make sure that the notice is available for individuals visiting the Provider for services, in the event that they ask for a copy.
6. The Provider will post the notice in a clear and prominent location within all medical offices, where it is reasonable to expect individuals seeking health care services to be able to read the notice.
7. Provider will prominently post the notice on any website(s) maintained by the Provider.

B. **Policy on Requested Restrictions on Uses and Disclosures**

1. Individuals have the right to request that the Provider limit its uses and disclosures of PHI in relation to treatment, payment and health care operations, or to request that the Provider not use or disclose PHI for these reasons at all. Such requests shall be made to the Provider in writing, using the Provider's Request for Restrictions form.
2. The Provider is not required to agree to a restriction requested by an individual. However, if the Provider does agree to a requested restriction, the Provider may not violate this restriction.
3. The Provider may terminate an agreed-to restriction by agreement with the individual, or by notifying the individual that the restriction will be terminated; provided that such termination is only effective with respect to PHI created or received after the Provider has so informed the individual, and that such termination is documented.

C. **Policy on Requests for Confidential Communications of PHI**

1. The Provider will take necessary steps to accommodate reasonable requests by individuals to receive communications of their PHI in an alternative, more confidential manner. Such requests shall be made during appointment check-ins.
2. The Provider will agree to confidential communications by alternative means or at alternative locations when presented with reasonable requests to do so.

D. **Policy on Access to PHI**

1. All patients have access to their PHI if they individually sign into their patient portals.
2. Individuals have the right to inspect and copy their PHI that the Provider or its business associates maintain. However, pursuant to federal law, individuals may not have access to the following: psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and PHI that is subject to federal or state law that prohibits access to that information. Denials based on these factors are not reviewable.
3. Access may also be denied to part or all of an individual's PHI if a licensed health care professional determines that such access is

reasonably likely to endanger or harm the individual or another person. Such denials are reviewable by an independent and licensed health care professional.

E. **Policy on Requests to Amend PHI**

1. The Provider shall provide individuals the right to request an amendment to their PHI that is created and maintained by the Provider or its business associates. Such requests shall be made in writing using the Provider's Request to Amend form.
2. The Provider may deny an individual's request for amendment if it determines that the requested PHI:
    a) was not created by the Provider, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the amendment;
    b) is not maintained by the Provider;
    c) would not be available for inspection under the Provider's Policy on Access to PHI; or
    d) is accurate and complete.
3. If a requested amendment is denied:
    a) The Provider will notify the individual in writing using the Provider's Denial of Amendment form.
    b) If the individual submits a statement of disagreement, the Provider may prepare a written rebuttal to the Statement of Disagreement. The Provider will provide the individual with a copy of any such rebuttal.
    c) The Provider will append or otherwise link the following to our records that is the subject of the disputed amendment:
        (1) the individual’s requisite for an amendment;
        (2) the denial of the request;
        (3) the individual’s statement of disagreement, if any; and
        (4) the Provider’s rebuttal, if any.

F. **Policy on Accounting for Disclosures**

1. The Provider shall, upon written request using the Provider’s Request for Accounting form, provide an individual with an accounting of our disclosures of the individual’s PHI, except for the disclosures:
    a) that relate to treatment, payment or health care operations;
    b) to the individual;
    c) made pursuant to a valid authorization;
    d) incidental to a permissible disclosure;
    e) provided for national security or intelligence purposes;
    f) made before April 14, 2003; or
    g) made more than six years prior to the request for accounting.
2. All disclosures that are required to be accounted for will be documented in the Provider's Electronic medical records. This will contain all information required for adequate accounting. The HIPAA Compliance Officer shall respond to a request for an accounting of disclosures by providing the individual with copies of Minimum Necessary/Disclosures for the time period requested by the individual, not to exceed six years, and not to cover dates earlier than April 14, 2003.
3. The Provider shall provide the first accounting in any 12-month period for free, but may charge the individual a reasonable, cost-based fee for further disclosures during that same 12-month period, provided that the individual has advance notice of the fee and has an opportunity to withdraw or modify the request to avoid or reduce

the fee.

VIII. Policy on Authorizations

A. For all uses and disclosures of PHI that are not described in Section Ill of this document, the Provider will obtain a signed authorization from the individual before making such disclosures.

B. The Provider shall not condition the provision of treatment on an individual's provision of an authorization unless, if deemed necessary within professional judgment, the provision of health care is solely for the purpose of creating PHI to a third party, in which case the treatment can be conditioned on obtaining an authorization for disclosure to such third party. This exception shall not apply with regard to PHI about psychotherapy notes, HIV/AIDS or treatment of alcohol and/or substance abuse or dependency.

IX. Policy on Business Associates

A. The Provider shall not share PHI with a business associate without first obtaining adequate assurances that the business associate will appropriately safeguard the information. Adequate assurances of safeguarding may only be obtained by executing a written business associate agreement with the business associate. The business associate agreement shall ensure that the business associate follow's Provider's privacy and security practices and otherwise complies with HIPAA in the course of any duties that involve use of PHI on behalf of Provider.

B. A business associate is any person or entity that performs a service for or on behalf of the Provider, where this service involves the use or disclosure of PHI.

C. If the Provider becomes aware that a business associate is in violation of the business associate agreement, the Provider will terminate the contract, or if termination is not feasible, the Provider will report the problem to the Secretary of Health and Human Services.

X. Policies Regarding the HIPAA Compliance Officer and Complaint Process

A. **Policy Regarding the HIPAA Compliance Officer.**

1. The Provider designates a HIPAA Compliance Officer as the person responsible for oversight of the policies and procedures regarding the privacy of health information, as well as for being the contact person who will receive complaints from individuals and answer their questions about the Provider's privacy policies and procedures. See Appendix A for the current contact information of the appointed HIPAA Compliance Officer.

B. **Policy Regarding our Complaint Process**

1. The Provider shall implement a process that allows individuals who believe that the Provider has not complied with these privacy policies to file a complaint with the HIPAA Compliance Officer.
2. Procedures.
    a) An individual who wishes to log a complaint with the Provider, alleging that the Provider has not complied with these privacy policies, shall file such complaint in writing to the HIPAA Compliance Officer.
    b) The HIPAA Compliance Officer shall investigate the complaint, but is under no obligation to report the results of this investigation to the individual, although the HIPAA Compliance Officer is encouraged to do so, since the

individual is permitted to file such complaints with the Secretary of the Department of Health and Human Services at any time.

c) The complaint and any documentation relating to the investigation or resolution of the complaint shall be maintained by the Provider for a period of not less than seven years.

XI. Policies on Workforce Training and Sanctions

A. **Policy on Workforce Training**

1. The Provider will train all workforce members who come into contact with PHI in the course of performing their duties on proper uses and disclosures of PHI, individual rights with regard to PHI, and all other policies that are relevant to their particular duties.

B. **Sanctions**

1. The Provider may impose appropriate sanctions against members of its workforce who fail to comply with these policies and procedures, on a fact specific basis.
2. Any sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use, or disclosure of PHI, and similar factors.
3. No sanctions shall be imposed under the following circumstances:
    a) file a complaint with the Department of Health and Human Services;
    b) testify, assist, or participate in an investigation, compliance review, proceeding, or hearing relating to compliance with the HIPAA Privacy Standards.
    c) oppose any act made unlawful by the HIPAA Privacy Standards; provided that the individual or person has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Standards; or
    d) disclose PHI as a whistleblower and the disclosure is to a health oversight agency, public health authority, or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity.

XII. Policy on Mitigating Violations

A. **Policy.** The Provider, upon discovering that a use or disclosure of PHI by a workforce member or business associate that is a violation of these policies and procedures, or of the HIPAA Privacy Standards, has had a harmful effect, shall mitigate, to the extent practicable, any resulting harmful effect that is known to the Provider.

B. **Procedures.**

1. Upon discovering that use or disclosure of PHI made by a workforce member or business associate that does not conform with these policies and procedures, or with the HIPAA Privacy Standards, has created a harmful effect, we shall determine what steps can be taken to mitigate this effect.
2. The Provider, after determining what steps can mitigate the harmful

effect, shall determine which of these steps is most practicable, and take such actions.

3. The Provider shall document in writing all determinations made and steps taken under this policy and its procedures, and retain such information for a period of seven years.

XIII. Policies on Non-Retaliation and Non-Waiver

A. **Policy on Non-Retaliation.** The Provider shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. any individual who exercises his or her right to:
    a) request access to their PHI;
    b) request amendments to their PHI;
    c) request an accounting of disclosures of their PHI;
    d) request confidential communications of PHI;
    e) request restrictions on the use or disclosure of their PHI;
    f) file a complaint, either to the Provider or to the Secretary of Health and Human Services for alleged violations of the HIPAA Privacy Standards; or
2. any individual or entity for:
    a) filing a complaint with the Secretary of Health and Human Services;
    b) testifying, assisting, or participating in an investigation, compliance review or hearing under the HIPAA Privacy Standards; or
    c) opposing any act or practice made unlawful by the HIPAA Privacy Standards, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Standards or these policies and procedures.

B. **Policy on Non-Waiver.** The Provider will not require an individual to waive their rights to file a complaint to the Secretary of Health and Human Services for perceived violations of the HIPAA Privacy Standards as a condition of payment for healthcare services, enrollment in the Provider, or eligibility for benefits.

XIV. Policy on Documentation

A. The Provider has implemented these written policies and procedures with respect to PHI, and these policies and procedures are designed to comply with the HIPAA Privacy Standards.

B. The Provider will maintain documentation, in written or electronic form, of these policies and procedures, as well as of all communications and other administrative documents required by these policies and procedures for a period of at least six years from the date of creation or the date when last in effect, whichever is later. This documentation shall include, but not be limited to, all authorization forms, business associate agreements, Privacy Notices and amendments thereto, and any correspondence sent to or received from individual patients relating to the use and disclosure of their PHI under these policies and procedures.

C. The Provider will incorporate into these policies, procedures and other administrative documents and changes in law, and shall properly document and implement any changes to policies and procedures as necessary pursuant to changes in law.

XV. HIPAA Security Policies

A. **Introduction and Purpose.** This policy addresses compliance with the HIPAA Security Rule. The Security Rule defines ePHI as protected health information in electronic form. Protected health information, in turn, means information that relates to the past, present or future physical or mental health or condition of an individual (including genetic information); the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

By implementing this policy Provider intends to:

- ensure the confidentiality, integrity, and availability of all ePHI Provider creates, receives, maintains, or transmits;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the HIPAA privacy rules; and
- ensure compliance by the Provider's workforce.

The policy takes into account Provider's:

- size, complexity, and capabilities;
- technical infrastructure, hardware, and software security capabilities;
- costs of security measures; and
- probability and criticality of potential risks to electronic protected health information.

While Provider is not responsible for the security of electronic transmissions it receives, Provider is responsible for the security and availability to authorized persons of ePHI after receipt, either while the data is at rest or during transmission.

B. **Administrative Safeguards**[1]

1. **Security Management Process.** Providers will prevent, detect, contain, and correct ePHI security violations.
2. **Risk Assessment Analysis.** Provider shall periodically conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI received and/or maintained by Provider . The analysis was carried out by Provider's HIPAA Compliance Officer, Security Officer and other IT personnel, as needed (collectively, the "Security Team").

Areas reviewed by the Security Team include:

- security processes (security administration, security monitoring, incident response, and virus detection);
- physical access to the data center and other critical operations areas;
- contingency planning;
- operating system and/or platform configurations;
- network configurations;
- data repositories;
- portal/web architecture; and
- risk analysis including threat assessment.

The Security Team has determined that the data items determined to qualify as ePHI, and

therefore impacted by this HIPAA Security Policy, include (i) email, electronic messages or other electronic transmissions containing patient names and other identifiers.

Provider's Security Team (with the assistance of outside vendors , as appropriate) prepares an Information Technology Risk Assessment on an annual basis. This assessment reviews risks associated with a number of key factors. These factors include, but are not limited to:

- security processes (security administration, security monitoring, incident response, and virus detection);
- physical access to the data center and other critical operations areas;
- contingency planning;
- operating system and/or platform configurations;
- network configurations;
- data repositories;
- portal/web architecture ; and
- risk analysis including threat assessment.

Provider then ranks the level of risk remaining after considering existing risk management factors. From this assessment, Provider identifies the key areas it will audit in the coming year.

3. **Risk Management.** Provider has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, and has documented identified risks, corrective actions taken, and risks considered acceptable as more fully described throughout this HIPAA Security Policy.
4. **Information System Activity Review.** The Provider will routinely monitor its IT systems relative to the use and dissemination of PHI and ePHI in accordance with its security practices.

C. **Assigned Security Responsibility.**[2]
   1. Security Officer responsibilities include the management and supervision of:
      a) the development and implementation of security measures to protect ePHI, and
      b) the conduct of personnel in using and protecting ePHI

D. **Assigned Workforce Security.**[3] Provider ensures that members of its workforce have appropriate access to ePHI, but that those who should not have access are restricted from such access. More specifically, access to Provider's IT system, on which ePHI is stored, requires user based authentication. This authentication system limits system access only to specified, authenticated individuals. Application level access is controlled by specific system user accounts, and they are password protected. All transactions involving and access to systems containing ePHI are logged locally as well as to a central auditing system. Firewall logs assess activity and monitor for suspicious activity. The various logs are periodically reviewed and analyzed for any evidence of electronic trespass, hacking or unauthorized attempts to access the IT system. With these measures in place, the risk of unauthorized access to ePHI is extremely low. Data on the IT system has never been compromised as of the date of this HIPAA Security Policy.

   Remote devices (laptops, smart phones, etc.) with access to Provider systems are encrypted and password protected. All employees who access Provider systems from personal remote devices agree in writing to ensure

appropriate access to such systems remotely, to install recommended antivirus applications, and to ensure that such devices are not accessed by third parties unaffiliated with Provider. In the event that such devices are lost or stolen, employees are required to immediately notify Provider IT personnel so that appropriate measures may be taken to protect Provider information accessible through such devices.

Appropriate measures will be taken upon a workforce member's termination, or if access otherwise needs to be removed, including: removal of all access to ePHI; account removal/disablement; lock access to personal files; and return of physical security items (e.g. cell phones, PDAs, blackberries, keys, laptops).

Accountability for completing terminations and assuring ePHI access is discontinued is properly assigned to the Security Team.

E. **Access.**[4] Provider controls and reviews access to ePHI. Provider has determined that the employees who access ePHI are as follows:
    1. All employees providing healthcare and related services for or on behalf of Provider's patients, also known as authorized personnel.
    2. Provider manages all user access to the IT system by ensuring that members of its workforce who need access to ePHI to do their jobs have appropriate access, while at the same time ensuring that those who should not have access to ePHI are restricted from such access

F. **Security Awareness.**[5] Provider shall provide ongoing security information training and awareness to employees who access ePHI through working with Provider. Training shall be conducted when employees are hired and annually thereafter.

    Training will, among other things, educate employees about processes for guarding against, detecting and reporting malicious software; discuss processes for monitoring IT system log-in attempts and reporting discrepancies; and discuss the necessity of creating, changing and safeguarding user accounts and passwords.

G. **Security Incident Procedures.**[6] Provider will address security incidents, which are the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

    Security incidents will be processed and documented by the Security Officer, which shall work in conjunction with local, state or federal agencies as needed.

    In the event of a security incident, affected systems shall be removed from the network and an exact copy of all data and appropriate logs on such systems shall be cloned. The original hardware, data and systems shall be shelved as evidence, and forensic analysis shall be performed on the cloned copies. All procedures and findings shall become written documents with controlled access.

    Recovery methods for compromised or affected systems shall include scanning of the machines and restoration of operating system(s) and data to pre-security incident state; provided, however, that if returning such

systems and date to a pre-security incident state is not possible, a complete rebuild of the affected system(s) shall be ordered.

H. **Contingency Plan.**[7] Provider has established policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems and facilities required to conduct business, including ePHI. In addition, all data is backed-up incrementally on a daily basis, and full back-ups are taken each week.

   These disaster recovery plans detail the responsibility of departmental supervisors to identify critical business activities and the required resources for resuming critical business in the event of an interruption like a disaster or other emergency. This includes hardware, software, and people resources for all areas. Recovery teams are identified and authorized to access data resources only as necessary to resume normal business operations. These disaster recovery plans are executed by employees that already have basic access as required by normal business and technical support duties. In the absence or shortage of these critical recovery staff, only authorized substitutes shall be given minimal access as required by restoration operations.

   All servers are on uninterruptible power supplies with sufficient hold time to permit data to be secured in the event of power loss. Back-up hardware is available under a disaster recovery plan. The Provider disaster recovery plan is attached to this Policy as Appendix B.

I. **Evaluation.**[8] Provider will annually perform an evaluation, based initially upon these standards, and later in response to environmental or operational changes affecting the security of ePHI, including:
   - risk analysis;
   - threat assessment;
   - operating system and network device security configurations;
   - access controls and authorization to ePHI;
   - security awareness;
   - security incident response;
   - physical security;
   - transmission security;
   - security model (i.e., data classification/ownership);
   - security policies/procedures; and
   - security architecture and design.

J. **Business Associates.** Administrative safeguards also apply to Provider's business associate/subcontractor contracts and other arrangements in which ePHI is handled on Provider's behalf. Such agreements will be negotiated into a written contract as more fully set forth in Subsection Rand the Privacy Policies.

K. **Facility Access Controls (Physical Safeguard).**[9] Provider limits physical access to electronic information systems and the facility in which they are housed, and ensures that only properly authorized access is allowed. This includes visitor and workforce authorization procedures appropriate to secure access to these facilities.

   The IT system and database servers where ePHI data are processed and stored are physically secured in monitored, climate controlled and locked

server rooms. Keys to the server room are controlled.

The Provider has developed a contingency plan that spells out processes to use during recovery from a disaster, including facility access in support of restoration of lost data under the disaster recovery plan and an emergency mode operations plan in the event of an emergency.

The Provider safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. This includes:

- periodic testing of the security of the computer rooms and sensitive areas;
- periodic review of the physical access lists; and
- environmental controls.

IT personnel have only "need to know" access to the areas and systems/data required by their jobs.

Provider maintains records of repairs and modifications to Providers network systems, and Provider destroys faulty hard drives before they leave Provider's facilities.

L. **Workstation Use and Security [10] (Physical Safeguard).** Employees who are permitted to access the IT system that houses ePHI do so via a confidential employee account with password protection. System access is audited and recorded. The system requires passwords to be routinely changed. Passwords must meet certain cryptographic standards, and old passwords may not be immediately reused.

M. **Device and Media Controls (Physical Safeguard).[11]** Provider maintains records of repairs and modifications to Provider's network systems, and Provider destroys faulty hard drives before they leave Provider's facilities.

It is the policy of Provider to erase all ePHI from electronic media before reusing or replacing the media.

The Provider keeps inventory records of which personnel are given access to which portable devices (such as laptops, PDAs, etc.)

N. **Technical Safeguards.[12]** Provider has purchased and implemented information systems that allow access only to those persons and/or software programs that have been granted access rights.

Provider has assigned a unique identifier for each employee who accesses ePHI, and this allows Provider to track and monitor the use of information systems containing ePHI.

Computer workstations automatically lock after ten (10) minutes of non-use, and users must enter their confidential password to re-enter the workstation.

Provider has implemented encryption technology for all emails containing PHI that are sent from Provider. The ZIXcorp program is available to all employees who use/disclose ePHI and who need to send ePHI via email to third parties as part of the Provider's normal operations. Although this program allows outside agencies to receive patient information securely, the preferred method of transmitting this information for The Wright Center is via fax.

O. **Audit Controls.[13]** Provider monitors and audits system access. Please see

Appendix C.

P. **Integrity.**[14] Provider utilizes secure tunneling technology to promote data integrity . Any email which might contain ePHI or other sensitive information will be transmitted by opening a hole in the network firewall to transport such information to only a particular endpoint and no other.

Q. **Person or Entity Authentication.** [15] Provider ensures that a person or entity seeking access to ePHI is the one claimed , and that access is only granted to Provider employees who require it for their jobs. All ePHI system users are assigned a user account, and are required to develop and periodically update a confidential password to access the system.

R. **Business Associate Contracts or other Arrangements.** [16] The contract or other arrangement between Provider and its patients or between Provider and its Business Associate(s), if any, meet the confidentiality requirements, as applicable. Any awareness of a pattern of an activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the contract or other arrangement will be immediately escalated, and will be considered a violation unless the Business Associate takes reasonable steps to cure the breach or end the violation; and if such steps are unsuccessful, terminate the contract or arrangement, if feasible.

   Contracts between Provider and its Business Associates require the Business Associates to implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on Provider's behalf. These safeguards must, in all instances, be no less protective of PHI and ePHI than the safeguards to which Provider is subject under its business associate agreements or that it is subject to as a Covered Entity.

   - Business Associates must ensure that any agent, including another subcontractor, to whom they provide such information agrees to implement safeguards to protect such information that are no less protective of PHI and ePHI than the safeguards to which such subcontractors are subject pursuant to their business associate agreements with Provider.
   - Any security incident or breach of which a Business Associate becomes aware must be reported to the Provider.
   - The Provider will regularly review current contracts to assess the need for amendment or re-contracting to ensure the implementation of HIPAA-compliant security practices with business associates or other subcontractors.

1 §164.308(a)(1)(i)
2 §164.308(a)(2)
3 §164.308(a)(3)(i)
4 §164.308(a)(4)
5 §164.308(a)(5)(i)
6 §164.308(a)(6)(i)
7 §164.308(a)(7)(i)
8 §164.308(a)(8)
9 §164.310(a)(1)
10 §164.310(b)
11 §164.310(d)(1)

§164.312(a)
§164.312(b)
§164.312(c)(1)
§164.312(d)
§164.314(a)(1)

REFERENCE
eCFR :: 45 CFR Part 164 -- Security and Privacy EOS© Toolbox

TAB 2

Date: _____/_____/20_____

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Authority/Identity Verification

Purpose: The purpose of this form is to determine the identity of any person or organization requesting access to an individual's protected health information, as well as the authority of such person or organization to access the information requested. Employees should complete this form in its entirety. If the requestor's identity and authority can be verified, then the employee should complete the Minimum Necessary/Disclosure Log form before delivering protected health information to the requestor.

1. Name of person requesting information: _____

2. Check if you are requesting in the capacity as an individual. ☐ (If not checked, go to #3)

- **If requesting as an individual, check the relationship with the patient:**

  ☐ Individual presented valid authorization
  ☐ Personal Representative
  ☐ Power of Attorney
  ☐ Guardian
  ☐ Family Member (specify: _____)
  ☐ Other (specify: _____)

- **Check if an individual's identity is verified by photo I.D.** ☐ (attach a copy of I.D.)
- **Attach** all documents provided to support the person's authority to access the PHI requested
- If unable to verify the requesting person's identity and/or authority to receive the PHI requested, or if there are any discrepancies discovered in verifying this person's identity or authority to access this information, **DO NOT** provide the requested information. Copy and attach the information provided by this person, comment in the space below on any shortcomings or discrepancies in the information provided, and forward all information to the HIPAA Privacy Officer immediately.
- **Employee comments:**
  _____
  _____

3. Check if requesting on behalf of a company, government entity, or other type of organization: ☐

- **Name of entity the person is requesting information for:**

  _____

- **Evidence of the person's authority to act on behalf of the entity:**
  - _____ Agency identification badge
  - _____ Statement on government letterhead
  - _____ Statement on organization letterhead (if not a government agency)
  - _____ Other (specify: _____)

- **Check if an individual's identity is verified by photo I.D.** ☐ (attach a copy of I.D.)

- **Evidence of entity's authority to access the requested PHI:**
  - _____ Authorization presented
  - _____ Warrant
  - _____ Subpoena
  - _____ Court order
  - _____ Other legal process (specify: _____)
- **Attach all documents provided to support the entity's authority to access the PHI requested.**
- **If unable to verify the requesting person's identity and/or the authority of his or her identity to receive the PHI requested, or if there are any discrepancies discovered in verifying the identity or authority of this person and entity to access this information, do NOT provide the requested information. Copy and attach the information provided by this person, comment in the space below on any shortcomings or discrepancies in the information provided, and forward all information to the Privacy Officer immediately.**
- **Employee comments:**

  _____

  _____

Employee Name (Printed): _____

Employee Signature: _____ *Date:* _____/_____/*20*_____

Check if reviewed by the Privacy Officer: ☐

Privacy Officer Signature: _____ Date: _____/_____/20_____

TAB 3

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Minimum Necessary/Disclosure Log

Purpose: The purpose of this form is to document our efforts to ensure that when we disclose an individual's protected health information to a third party, only the minimum necessary information is disclosed. Additionally, documenting such disclosures on this form will enable **The Wright Center for Community Health** to efficiently comply with an individual's request for an accounting of disclosures of their protected health information. Employees who release information to third parties following the required minimum necessary determination should complete this form in full, and submit it to the Privacy Officer.

Section A: Individual Information

Date: _____

Name of the individual whose protected health information was disclosed: _____

Address:_____

Telephone: _____ E-mail: _____

Date of Birth: _____

Social Security Number: _____ - ____ - _____

Section B: Disclosure Information

Date of the disclosure: _____/_____/20_____

Name and address of person and/or entity to whom the protected health information was disclosed:
_____
_____

Describe the protected health information disclosed: _____
_____

Did the recipient of the protected health information have authorization?

Yes ☐ (attach authorization to this form) No ☐

If no authorization was furnished, describe the purpose for disclosing the protected health information:
_____
_____
_____

Is this disclosure one of a series of repetitive disclosures to the same person/entity or for the same purpose to the individual listed in Section A? Yes ☐ No ☐

If yes, state the date of the first disclosure of the series and the frequency or number of these repetitive disclosures made prior to the disclosure being reported on this form: _____
_____

Section C: Minimum Necessary Determination (check all that apply)

☐ No minimum necessary determination applies to this disclosure because:

☐ The disclosure was to the individual in Section A or to that individual's personal representative

☐ The disclosure was requested or authorized by the individual in Section A or that individual's personal representative. Attach the authorization.

☐ The disclosure was in response to an authorization received from a covered entity (a health plan, health care provider, or a clearinghouse), and we have no reason to believe that the covered entity requested more than the minimum necessary.

☐ The disclosure was to a public official who represented that the request is for the minimum necessary, and we have no reason to disbelieve the representation.

☐ The disclosure was to a professional, such as a lawyer or accountant, who is either a member of **[**_____ **]**'s workforce or a business associate, and who represented that the request is for the minimum necessary, and we have no reason to disbelieve the representation.

☐ The disclosure was to a researcher who provided appropriate documentation from the Institutional Review Board or other approval entity to support the disclosure.

☐ The disclosure was to a health care provider to carry out treatment.

☐ The disclosure was to the Department of Health and Human Services for compliance review or complaint investigation.

☐ The disclosure was required by law. Cite the law: _____

☐ The disclosure was required for compliance with HIPAA Administrative Simplification Rules. Cite the rule and why the disclosure was required to comply with it: _____
_____

☐ This disclosure was part of a series of routine or recurring disclosures, and **[** _____ **]** has determined that these disclosures are the minimum necessary for the purposes stated above. This determination was:

☐ made in conjunction with the completion of this form by the following individual and on the following date: _____

☐ previously made pursuant to the original of the routine/recurring disclosures by the following individual on the following date: _____

☐ This disclosure was the minimum necessary for the stated purpose based on an individualized determination made by the following individual on the following date: _____
_____

☐ This disclosure was for an entire medical or clinical record. State the justification for the entire medical record being the minimum necessary protected health information for the purpose:
_____
_____

SIGNATURE

I attest that the above information is correct.

Signature: _____ Date: _____/_____/20_____

Print Name: _____ Title: _____

Attach the completed Authority/Identity Verification Form and all applicable authorizations to this Minimum Necessary/Disclosure Log and submit it to the Privacy Official. Retain a copy for your department's records.

TAB 4

THE WRIGHT CENTER FOR COMMUNITY HEALTH

NOTICE OF PRIVACY PRACTICES

This Notice Describes:

- HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED
- YOUR RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION
- HOW TO FILE A COMPLAINT CONCERNING A VIOLATION OF THE PRIVACY OR SECURITY OF YOUR HEALTH INFORMATION OR OF YOUR RIGHTS CONCERNING YOUR INFORMATION

YOU HAVE A RIGHT TO A COPY OF THIS NOTICE (IN PAPER OR ELECTRONIC FORM) AND TO DISCUSS IT WITH THE DIRECTOR OF CLINICAL COMPLIANCE ("DCC") AT 570.343.2383 EXT. 1699 OR AT twc-compliance@thewrightcenter.org IF YOU HAVE ANY QUESTIONS.

I. Who We Are.

This patient notice ("Notice") describes the privacy practices of The Wright Center for Community Health and The Wright Center for Graduate Medical Education ("TWC"). This Notice is prepared in accordance with the regulations governing the privacy of substance use disorder ("SUD") treatment records found at 42 C.F.R. Part 2 ("Part 2"). TWC reserves the right to change the terms of this Notice and to make the new notice provisions effective for records that it maintains. If TWC revises this Notice, it will provide you with a copy by posting it on our website and at clinic locations. It will also provide a copy of the then-current Notice upon request.

While treating you, our employees, volunteers, students, and health care professionals affiliated with TWC follow this Notice. In addition, any person involved in your care, entities, sites, and locations may share medical information about you with each other for treatment, payment, or health care operations as described in this Notice.

We are required by law to maintain the privacy of your health information and to provide you with this Notice.

II. Our Duties to Safeguard your Protected Health Information.

Protected Health Information ("PHI") is any information related to your health care that is shared or maintained in any manner. It includes your insurance information as well. This Notice applies to all PHI generated by TWC. Non-TWC physicians may have different policies or notices regarding the physician's use and disclosure of your medical information created in the physician's office.

This Notice will tell you about the ways in which we may use and disclose your PHI. We also describe your rights and certain obligations we have regarding the use and disclosure of your PHI.

We are required by law to:

- ► maintain the privacy of your PHI and SUD Records (defined below);
- ► to provide you with this Notice;
- ► follow the terms of the Notice that is currently in effect; and

- ► to notify you following a breach of any unsecured versions of SUD Records.

III. **How The Wright Center May Use and Disclose Medical Information About You - Treatment, Payment, and Health Care Operations.**

Single Consent. Except in an emergency or other special situations, you may provide a single consent for all future uses or disclosures of SUD Records to your treating providers, health plans, third-party payers, and people helping to operate TWC's program for the purposes of treatment, payment, and/or health care operations pursuant to Part 2, so that we may use and disclose your PHI and/or SUD Records for the following purposes:

Treatment. We may use and disclose PHI and/or SUD Records about you in connection with your treatment, for example, to diagnose you. In addition, we may contact you to remind you about appointments, give you instructions prior to tests or surgery, or inform you about treatment alternatives or other health-related benefits or services. We may also disclose your PHI and/or SUD Records to other providers, doctors, nurses, technicians, medical students, clinical personnel, or other health care facilities or entities for treatment, care coordination or quality improvement activities. We will communicate this PHI and/or SUD Records using phone, fax, two-way radio, or electronic transfer.

Payment. We may use and disclose your PHI and/or SUD Records to obtain payment for services we provide to you. For example, we may contact your insurance company to pay for the services you receive, to verify that your insurer will pay for the services, to coordinate benefits, or to collect any outstanding accounts.

Health Care Operations. We may use and disclose your PHI and/or SUD Records for health care operations, which include activities related to evaluating treatment effectiveness, teaching and learning purposes, evaluating the quality of our services, investigating complaints related to service, fundraising activities, and marketing activities. An Accountable Care Organization (ACO) is a group of physicians, hospitals, and other health care providers that come together voluntarily to give coordinate care to Medicare beneficiaries. TWC participates in ACOs and other value-based entities from time to time, so TWC may share PHI with providers within the ACO or other value-based entities for purposes such as evaluating outcomes and ensuring quality care.

Other Health Care Providers. We may also disclose your PHI and/or SUD Records to other health care providers when such PHI and/or SUD Records are required for them to treat you, receive payment for services you receive, or conduct certain health care operations. For example, we will share your PHI and/or SUD Records with an ambulance company so the ambulance company can be reimbursed for transporting you.

Health Information Exchange. A health information exchange ("HIE") is a network that allows HIE participants to share patients' PHI and/or SUD Records for treatment, payment, and healthcare operations purposes and other lawful purposes to the extent permitted by law ("Permitted Purposes"). HIEs make it possible for us to electronically share patients' PHI and/or SUD Records to coordinate care, obtain billing information, and participate in quality improvement, public health, and population health initiatives, among other things. Participants in the HIE may be healthcare providers, their billing companies, insurers, health plans, and accountable care organizations ("Participants"). Note that sensitive information (such as information relating to mental health, drug and alcohol treatment, HIV status, and

sexually transmitted diseases) may be contained in the documents accessed through the HIE.

TWC participates in HIEs from time to time solely for the Permitted Purposes, including KeyHIE. More information on KeyHIE can be found on its website: https://www.keyhie.org/.

Opting Out of HIEs. You may opt out of participating in all of the HIEs TWC participates in by contacting the TWC [DCC] or by going to this link and completing the opt-out form:https://thewrightcenter.org/wp-content/uploads/2025/03/HIE-Opt-Out-Form-1.pdf. KeyHIE's policy regarding privacy and security is at https://www.keyhie.org/about-us/compliance.

IV. Other Uses and Disclosures of Your PHI for which Authorization is Not Required.

Unless TWC has a consent signed by you, it may only disclose records related to you that are maintained now or in the future by TWC in its electronic health record including, but not limited to, SUD treatment records—except, subject to certain exceptions, SUD counseling notes—("SUD Records") in accordance with the limited circumstances permitted by Part 2 related to:

Disclosure to Relatives and Close Friends. We may disclose your PHI to a family member, other relative, a close personal friend or any other person if we: 1) obtain your agreement; 2) provide you with the opportunity to object to the disclosure; or, 3) we can reasonably infer that you do not object to the disclosure. Disclosure of SUD Records is subject to a stricter standard.

Incapacity or Emergency Circumstances. If you are not present, or the opportunity to agree or object to a use or disclosure cannot practicably be provided because of your incapacity or an emergency circumstance, we may exercise our professional judgment to determine whether a disclosure of PHI to relatives and/or close friends is in your best interest (disclosure of SUD Records is subject to a stricter standard). If we disclose information to a family member, other relative, or a close personal friend, we would disclose only information that is directly relevant to the person's involvement with your health care.

Fundraising. We may contact you to request a contribution to support important activities of TWC or its foundation. In connection with any fundraising, we may use and disclose your demographic information as well as the dates on which you received health care services, the department where you received your services, your treating physician, and outcome information related to your care. If you do not want to receive any fundraising requests, you may contact us at twc-compliance@thewrightcenter.org or:

Director of Clinical Compliance
The Wright Center for Community Health
501 S. Washington Avenue, Suite 1000
Scranton, PA 18505

Public Health Activities. We may disclose your PHI and/or SUD Records for public health activities under certain circumstances, including the following:

- ► Reporting births or deaths
- ► To prevent or control disease, injury, or disability
- ► To report child abuse or neglect
- ► To report reactions to medications or problems with products

- ► To notify individuals who may have been exposed to a disease or may be at risk for contracting a disease or condition
- ► Reporting PHI and/or SUD Records to your employer as required by laws addressing work-related illnesses and injuries or workplace medical surveillance

Victims of Abuse, Neglect or Domestic Violence. If we reasonably believe you are a victim of abuse, neglect or domestic violence, in accordance with current Pennsylvania law, we may disclose your PHI and/or SUD Records to a governmental authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence.

Health Oversight Activities. We may disclose your PHI and/or SUD Records to a health oversight agency that is responsible to ensure compliance with rules of government health programs such as Medicare and Medicaid. These oversight activities include, for example, audits, investigations, inspections and licensure.

Legal Proceedings and Law Enforcement. PHI and/or SUD Records, or testimony relaying the content of such records, will not be used or disclosed in any civil, administrative, criminal, or legislative proceedings against you unless based on specific written consent or a court order. Records will only be used or disclosed based on a court order after notice and an opportunity to be heard is provided to you and/or TWC as the holder of the record required by Part 2 and 42 U.S.C. 290dd-2, which are a federal statute and set of regulations that, among other things, protect the privacy of SUD treatment records. A court order authorizing use or disclosure must be accompanied by a subpoena or other similar legal mandate compelling disclosure before the record is used or disclosed.

Deceased Persons. We may release PHI to a coroner or medical examiner authorized by law to receive such information.

Organ and Tissue Donation. We may disclose your PHI and/or SUD Records to organizations that obtain organs or tissues for banking and/or transplantation.

Public Safety. We may use or disclose your PHI and/or SUD Records to prevent or lessen a serious or imminent threat to the safety of a person or the public.

Research. Usually, we will ask for your permission or authorization before using your PHI and/or SUD Records for research purposes. However, we may use and disclose your PHI and/or SUD Records without your authorization if a qualified Institutional Review Board ("IRB") has waived the authorization requirement. An IRB is a committee that oversees and approves research involving human subjects.

Disaster Relief Efforts. We may disclose your PHI and/or SUD Records to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status, and location.

Military, National Defense, and Security. We may release your PHI and/or SUD Records if required for military, national defense and security, and other special government functions.

Workers' Compensation. We may release your PHI and/or SUD Records for workers' compensation or similar programs. These programs provide benefits for work-related injuries

or illnesses.

Communications from Us. We may use or disclose your PHI and/or SUD Records to identify health-related services and products that may be beneficial to your health, such as notification of a new physician and/or additional products and services, and then contact you about those products and services. If you do not wish to receive information of this type, please contact us at twc-compliance@thewrightcenter.org or:

Director of Clinical Compliance
The Wright Center for Community Health
501 S. Washington Avenue, Suite 1000
Scranton, PA 18505

As Required by Law. We may use and disclose your PHI and/or SUD Records when required to do so by any other laws not already referenced above.

V. Uses and Disclosures Requiring Your Specific Authorization.

Highly Confidential Information. Federal and State laws require special privacy protections for certain highly confidential information about you. This includes PHI that is: 1) maintained in psychotherapy notes or SUD counseling notes; 2) documentation related to mental health or developmental disabilities services; 3) drug and alcohol abuse, prevention, treatment and referral information; and, 4) information related to HIV status, testing and treatment as well as any information related to the treatment or diagnosis of sexually transmitted diseases. Generally, we must obtain your authorization to release this type of PHI. However, there are limited circumstances under the law when this type of PHI may be released without your consent. For example, certain sexually transmitted diseases must be reported to the Department of Health.

Other Uses or Disclosures Not Described in This Notice. Other uses and disclosures of PHI and/or SUD Records not covered by this Notice or permitted under the laws that apply to us will be made only with your written permission. Except as permitted under this Notice or as permitted by law, we will seek your written permission prior to using or sharing your information for marketing purposes or selling your information.

Revocation. Even after you give consent, you have the right to revoke that consent at any time in writing delivered to the address contained in this Notice or to the following email address: twc-compliance@thewrightcenter.org. After TWC receives your written notice to revoke, it will terminate your earlier consent within five business days. Prior to such termination, TWC may have shared some or all of my information or otherwise taken action in reliance on your consent; neither the organization nor any of its representatives are liable for any release of information during such time.

VI. Your Rights Regarding Medical Information About You.

You have the following rights regarding PHI and/or SUD Records we maintain about you as provided in Part 2. To exercise any of the following rights, please contact DCC in person, via mail, via telephone, or via email using the contact information on the first page of this Notice. Include a description of the right that you wish to exercise, a description of how you wish to exercise it, and your contact information so that we may contact you with questions.

Right to Obtain. You have the right to request your PHI and/or SUD Records, excluding psychotherapy notes or SUD counseling notes, in a hard-copy or electronic format if we maintain the PHI and/or SUD Records in an electronic format. You may be charged a fee for the costs of copying, mailing or other supplies associated with your request. Instructions on how to request your PHI are at: https://thewrightcenter.org/corporate-policies/

Right to Inspect and Copy. You have the right to inspect and copy PHI and/or SUD Records that may be used to make decisions about your care, excluding psychotherapy notes and SUD counseling notes. Instructions on how to request your PHI are at: https://thewrightcenter.org/corporate-policies/

We may deny your request to inspect and copy in certain very limited circumstances. You may request a professional review of the denial. If you request a review, then we will designate another TWC-licensed healthcare professional to review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

Right to Amend. You have the right to request that we amend the PHI and/or SUD Records we keep about you in your medical and billing records. Instructions on how to request an amendment to your PHI are at: https://thewrightcenter.org/corporate-policies/

We will ask your provider(s) to review amendment requests to the medical record. We may deny your request if we believe the information you wish to amend is accurate, current, and complete without your requested amendment, or the PHI was not created by TWC, or other special circumstances apply.

Right to an Accounting of Disclosures. You have the right to request a record of all disclosures of your PHI and/or SUD Records in electronic form for the past 3 years and a right to an accounting of disclosures as set forth in the HIPAA regulations for all other disclosures made with consent.

To request this list or accounting of disclosures, you must submit your request in writing to:

Director of Clinical Compliance
The Wright Center for Community Health
501 S. Washington Avenue, Suite 1000
Scranton, PA 18505
570.343.2383, ext. 1699

Right to Request Restrictions. You have the right to request restrictions of disclosures made with prior consent for purposes of treatment, payment and health care operations. We are not required to agree to your request. If we agree to a restriction, we will abide by restrictions unless a disclosure is needed to provide you emergency treatment.

You also have the right to request a restriction of disclosure of your PHI and/or SUD Records to your health plan for those services for which you have paid in full. If you request we not share your PHI and/or SUD Records with your medical insurer or other third-party payer, we will honor your request, provided you pay in full for the health care item or service.

To request restrictions, you must make your request in writing to the appropriate TWC office or department. In your request, you must tell us: 1) what information you want to limit; 2) whether you want to limit our use, disclosure, or both; and 3) to whom you want the limits to apply, for example, disclosures to your spouse. Instructions on how to request a restriction(s) to your PHI are at: https://thewrightcenter.org/corporate-policies/

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. To request confidential communications, you must make your request in writing to the appropriate TWC office or department. We will accommodate reasonable requests. Your request must specify how or where you wish to be contacted. Instructions on how to request a Confidential Communications regarding your PHI are at: https://thewrightcenter.org/corporate-policies/

Right to Revoke Your Authorization. You may revoke your authorization for us to use and disclose your PHI and/or SUD Records at any time by submitting a request in writing to the appropriate office or department.

Right to List. You have a right to a list of disclosures by an intermediary for the past 3 years. To request such a list, you must make your request in writing to the appropriate TWC official or department. Your request must specify the disclosing intermediary.

Notice. You have the right to obtain a paper or electronic copy of this Notice upon request. To request this Notice, you must make your request to the appropriate TWC official or department and specify if you wish to receive this Notice in paper or electronic format.

You also have the right to discuss and ask questions about this Notice. Questions should be directed to the appropriate TWC official.

Fundraising. You have the right to elect not to receive fundraising communications, as discussed above.

Complaints. You have the right to submit a complaint to TWC and to the Secretary of the Department of Health and Human Services if you believe your privacy rights have been violated, as discussed in more detail below. You will not be retaliated against for filing a complaint.

VII. Changes to This Notice.

We reserve the right to change this Notice. Revised Notices will be posted in appropriate locations and online at thewrightcenter.org/corpotate-policies. We reserve the right to make the revised or changed Notice effective for medical information we already have about you as well as any information we receive in the future. A copy of the current Notice is available upon request.

VIII. Complaints.

If you believe your privacy rights have been violated, you may file a complaint in writing with the TWC DCC at:

Director of Clinical Compliance

The Wright Center for Community Health
501 S. Washington Avenue, Suite 1000
Scranton, PA 18505
570.343.2383, ext. 1699

You may also wish to file a complaint with the Office for Civil Rights of the U. S. Department of Health and Human Services.

https://www.hhs.gov/ocr/complaints/index.html

We will not penalize you if you file a complaint.

IX. Breach Notification.

We will notify you in the event of a breach (as defined by HIPAA) of your PHI and/or SUD Records.

This Notice is effective: March 1, 2025

NOTICE OF NONDISCRIMINATION

Discrimination Is Against the Law

The Wright Center for Community Health complies with applicable Federal civil rights laws and does not discriminate or exclude people on the basis of race, religion, color, national origin, ancestry, age, disability, sex, parental status, political affiliation, military service, or relationship status.

The Wright Center:

► Provides free aids and services to people with disabilities to communicate effectively with us, such as qualified sign language interpreters;

► Provides free language services to people whose primary language is not English, such as qualified interpreters and information written in other languages.

If you need these services, contact The Wright Center for Community Health at 570.230.0019.

If you believe that The Wright Center has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with:

Senior Vice President, Executive Counsel and Chief Governance Officer
The Wright Center for Community Health
501 S. Washington Avenue, Suite 1000
Scranton, PA 18505
Phone: 570.343.2383 Fax: 570.963.6133
Email: walshj@thewrightcenter.org

If you need help filing a grievance, TWC Patient Advocacy is available to help you. You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights electronically through the Office for Civil Rights Complaint Portal, available at http://ocrportal.hhs.gov/ocr/portal/lobby.jsf, or by mail or phone at:

U.S. Department of Health and Human Services; 200
Independence Avenue, SW
Room 509F, HHH Building; Washington, DC 20201
1-800-368-1019 1-800-537-7697 (TDD)
Complaint forms are available at: http://www.hhs.gov/ocr/office/file/index.html

ATTACHMENT B

Acknowledgment of Receipt of Notice of Privacy Practices

By signing below, I acknowledge receipt of the *Notice of Privacy Practices* of The Wright Center for Community Health ("TWC"). In addition, by signing below, I authorize TWC to disclose my health information in conformance with the provisions of the Notice of Privacy Practices.

_____	_____
Signature of Patient	Signature of Personal Representative
_____	_____
Patient Name – PRINT	Personal Representative Name - PRINT
_____	_____
Date / Time	Date / Time
	_____
	Relationship to Patient

Inability to Obtain Acknowledgement

(To be completed only if no signature is obtained)

No acknowledgment of receipt of the Notice of Privacy Practices was obtained from the patient because:

- □ The individual refused to sign
- □ Communication barriers prohibited obtaining the acknowledgment
- □ An emergency situation prevented us from obtaining the acknowledgment
- □ Other (Please specify): _____

_____

_____	_____
Signature of TWC Representative	Date / Time

Rev. 07/2024

TAB 5

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Individual Request for Restrictions on Uses and Disclosures of Protected Health Information

As provided by regulations promulgated by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996, you have a right to request restrictions on how we use and disclose medical information we maintain about you. This information is called "protected health information."

We are not required to agree to your requested restriction, but we will make every effort to agree to any reasonable request. If we agree to your request, we will honor it, unless your protected health information is needed to treat you in an emergency medical situation. Also, please note that any restriction on use or disclosure of your information that we agree to will *not* apply in the following instances:

- When you access your own protected health information;
- Where you request an accounting of how we have used or disclosed your protected health information;
- Where we have included certain protected health information in our facility directory pursuant to your agreement to this use; or
- Where we make disclosures for certain specialized purposes, such as judicial or administrative purposes; health oversight; law enforcement; public health; to avert a serious threat to health and safety; decedents; Workers' Compensation; victims of abuse, neglect or domestic violence; specialized government functions; as required by law; or cadaveric organ, eye, eye or tissue donation.

Please describe how you would like TWCCH to restrict our use and disclosure of your protected health information:

_____
_____
_____
_____

We will notify you within thirty days of this request as to whether we agree to your requested restriction.

_____ _____/_____/_____
Print Patient Name Patient Date of Birth (DOB)

_____ _____/_____/20_____
Patient Signature Date

_____ _____ _____/_____/20_____
Received by Employee (print) Employee Signature Date

Employees must submit this form to the Privacy Officer, retaining a copy for department records.

Revised: January 20, 2025

TAB 6

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Individual Request for Confidential Communications
of Protected Health Information

Date: _____

As provided by regulations promulgated by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996, you have a right to request that we share your medical information with you through alternative and confidential means or at alternative locations. For example, you might ask that we send certain information to a particular address or that we use an envelope marked "confidential."

If you would like to make such a request, you must do so in writing by completing this form. We are not permitted to require that you provide us with a reason for your request. We will honor all requests to the extent that they are reasonable. If we deny a request, you will be notified in writing with a full explanation of our denial.

Please describe in detail how you would like TWCCH to communicate with you about your medical information. Please provide specific details with regard to ***where*** you would like us to communicate with you (i.e. particular addresses or telephone numbers, etc.) and ***how*** you would like us to communicate with you (i.e.: mail, email, telephone, whether mailings should be marked in a particular way, etc.):

_____
_____
_____
_____

We will notify you within thirty days of this request as to whether we agree to your requested restriction.

_____ _____/_____/_____
Print Patient Name Patient Date of Birth (DOB)

_____ _____/_____/20_____
Patient Signature Date

_____ _____ _____/_____/20_____
Received by Employee (print) Employee Signature Date

Employees must submit this form to the Privacy Officer, retaining a copy for department records.

Revised: January 20, 2025

TAB 7

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Individual Request for Access to
Protected Health Information

Date: _____

As provided by regulations promulgated by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996, you have a right of access to inspect and obtain a copy of your protected health information maintained by us. This right does not apply to:

1. Psychotherapy notes, which are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session, that are maintained separately from the rest of the patient's medical record.
2. Information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding; and
3. Where access to the information would violate the Clinical Laboratory Improvements Amendments of 1988.

Please indicate specifically the information that you would like to access:
_____
_____

TWCCH will act on this request within 30 days of the date we receive the request within 60 days if the requested information is not maintained or accessible to TWCCH on-site. Such action will either inform you of the acceptance of the request and provide you with the requested access or provide a written denial explaining the reasons for the denial and whether you are entitled to have the denial reviewed.

If the requested information is contained in more than one set of records or at more than one location, and access is granted, then TWCCH needs only to provide you with access to information contained in one of the record sets.

Please indicate the format you would like to receive your requested information (i.e. - paper, CD, USB drive, etc):
_____

Please indicate how you wish to inspect or obtain a copy of the requested information (i.e., fax, mail, on-site, etc., and provide the necessary numbers and/or address):
_____

If TWCCH cannot readily produce the information in the form or format you have requested, such information will be made available to you in a readable hard copy form or other form or format agreed to.

Do you agree to receive a summary of the requested information in lieu of access?

☐ Yes ☐ No

TWCCH may impose a fee as allowed by law to cover the cost of labor, copying, postage, and preparing a summary of the requested information. I agree to such fees imposed by TWCCH for providing a copy or summary of the requested information.

☐ Yes

_____		_____/_____/_____
Print Patient Name		Patient Date of Birth (DOB)
_____		_____/_____/20_____
Patient Signature		Date
_____	_____	_____/_____/20_____
Received by Employee (print)	Employee Signature	Date

****Forward this form to the Privacy Officer and retain a copy for department records.**

Date: _____/_____/20_____

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Denial of Access to
Protected Health Information

_____ _____/_____/_____
Patient Name Patient Date of Birth (DOB)

We have reviewed your request for access to your medical records. We are denying your request for the following reasons:

☐ We do not maintain the information you requested. That information is maintained by the entities listed below. You have no right to appeal this denial.
_____

☐ Part of the information you requested is not contained in our records. Accordingly, we are not required to provide it to you, and you have no right to appeal this denial. However, we will provide you with access to that part of the information you requested that is in our records. This information includes:
_____

☐ We are not required to release the information you requested because:

- ☐ You requested psychotherapy notes.
- ☐ The information requested has been compiled by us in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- ☐ Granting you access to the requested information would violate the Clinical Laboratory Improvements Amendments of 1988.

You have no right to appeal this denial

- ☐ We have determined that release of the information you request may result in harm to you or someone else.

You have the right to have this denial reviewed by a Licensed Healthcare Professional designated by The Wright Center for Community Health to act as a reviewing official who did not participate in the original denial decision.

You may exercise your right of review by submitting the attached Request for Review form with the Privacy Officer, whose telephone number appears below, within 60 days of the date of this denial.

You may also submit a complaint about this denial of access to the Secretary of the U.S. Department of Health and Human Services. Your complaint must be in writing, either on paper or electronically, and must include the following information: (1) our name and (2) a description of the acts or omissions that you believe violate our responsibilities under the federal Privacy Rule. Your complaint must be filed within 180 days of the date of this denial.

_____ _____
Privacy Officer Telephone

_____
Date

Revised: January 20, 2025

TAB 8

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Denial of Request to Amend
Protected Health Information

Date: _____/_____/20_____

Name:_____

Date of Birth: _____

Address:_____

Telephone: _____ E-mail: _____

Social Security Number: _____

We have reviewed your request for amendment to your medical records. We are denying your request for the following reasons:

☐ We do not maintain the information you requested.

☐ We did not create the records you wish to amend, and we have no basis to believe that the person or entity that did create the records is no longer available to amend them.

☐ We believe the records you wish to amend are complete and accurate.

☐ The records you asked to amend are not subject to your right to amend because they are psychotherapy notes, or have been compiled in anticipation of a civil, criminal or administrative action or proceeding.

You may indicate your disagreement with our denial by submitting a Statement of Disagreement Form to the Privacy Officer. If you do, we will append or link your statement to the records you wanted amended (if we have those records) for inclusion in future disclosures of those records. We may prepare and send you a rebuttal to your Statement of Disagreement and, if we do, we will append or link our rebuttal to those same records for inclusion in future disclosures of those records. Alternatively, we may substitute an accurate summary of your written statement and our rebuttal with future disclosures of those records.

If you do not submit a statement of disagreement, then you may request that we provide your Request for Amendment and our Denial with any future disclosures of your health information. Alternatively, we may substitute an accurate summary of your Request and our Denial with such disclosures.

You may also submit a complaint about our Denial of your Request to Amend your health information to the Secretary of the U.S. Department of Health and Human Services. Your complaint must be in writing, either on paper or electronically, and must include the following information: (1) our name, and (2) a description of the acts or omissions that you believe violate our responsibilities under the federal Privacy Rule. Your complaint must be filed within 180 days of the date of this denial.

Should you have any questions, please call the Privacy Officer at 570-343-2383 x1699.

_____ _____
Signature Print Name

Revised: January 20, 2025

_____
Date

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Individual Request for Amendment to
Protected Health Information

- Please complete and submit this form to request an amendment to the health information about you that we maintain in our records.
- Date: _____

SECTION A: Individual requesting records amendment.

Name:_____

Date of Birth: _____

Address:_____

Telephone: _____ E-mail: _____

Social Security Number: _____

SECTION B: Request that information be amended.

You have the right to request that we amend health information in our records and those of our business associates. We may deny your request if we do not maintain the information you seek to amend, if we did not create the information (unless you provide us with a reasonable basis to believe that the originator of PHI is no longer available to act on the amendment), if we believe the information is complete and accurate, or if the information consists of psychotherapy notes or information compiled in anticipation of civil, criminal or administrative proceedings. To request an amendment of your health information, please provide the following information:

Please specify the records you wish to amend and the amendments you wish to make:

_____
_____
_____

Please state the reasons for the amendments:

_____
_____

Please list the name and address of each person who you want us to notify of the amendment should we agree to make the amendment you request. You must provide us with a signed authorization for us to notify these persons. We can supply you with the appropriate authorization form.

_____ _____

_____ _____

_____ _____

Signature Date

Effective: 11/2018

Revision: 09/2024; Reviewed: 01/2025

TAB 9

THE WRIGHT CENTER for COMMUNITY HEALTH

Individual Request for an Accounting of Disclosures
Protected Health Information

Date: _____

Please complete and submit this form to request an accounting of our disclosures of health information about you that we maintain in our records. We will respond to your request within sixty (60) days, unless we send you notification that we will require an additional thirty (30) days to process your request. Please note that we will not account for the following:

- disclosures that relate to your treatment, payment or health care operations;
- disclosures directly to you;
- disclosures made pursuant to a valid authorization signed by you;
- disclosures that are incidental to a permissible disclosure;
- disclosures that were for a facility directory or to persons involved in your care, for which you were given the opportunity to agree or object;
- disclosures provided for national security, intelligence or law enforcement purposes;
- disclosures made before April 14, 2003; or
- disclosures made more than six years ago (or three years ago, in the event that we have disclosed information from an electronic health record).

SECTION A: Individual requesting records accounting.

Name: _____

Date of Birth: _____

Address: _____

Telephone:_____

E-mail:_____

Social Security Number: _____

SECTION B: Request for accounting.

Please indicate the dates for which you would like an accounting of disclosures (note that we will not account for disclosures made before April 14, 2003, or disclosures that were made more than six years ago):

_____/____/_____ through ____/____/_____

You are entitled to one free accounting of disclosures during each twelve-month period. Therefore, if this is your first request for an accounting of disclosures during the last twelve months, we will provide this service free of charge. However, if you have requested additional accountings over the last twelve months, we are permitted by law to levy a reasonable, cost-based charge for providing this accounting.

_____ _____

Signature Date

TAB 10

THE WRIGHT CENTER FOR COMMUNITY HEALTH

Pt Name _____

DOB _____

MR # _____

Patient ID

Section I: PATIENT INFORMATION

I hereby authorize THE WRIGHT CENTER to release medical information from the records of:

Patient Name: _____ D.O.B.: _____

Address: _____ Phone: _____

City/State/Zip Code: _____

Covering the period(s) of care (list applicable dates of treatment): _____

Section II: PURPOSE OF DISCLOSURE AND INFORMATION TO BE DISCLOSED

Information to be disclosed (check all applicable items to be released):

(May include Mental Health and/or Substance Use Disorder Information)

☐ History and Physical	☐ Therapist Notes	☐ Discharge Records / Summary	☐ Progress Notes
☐ Intake Documentation	☒ Entire record	☐ Medication Information	☐ Diagnosis code
☐ Psychiatric Evaluation	☐ Treatment Plans	☐ Imaging	☐ Labs
☐ Dental	☐ Immunizations		

Other (please specify): _____

_____

_____

I understand that any information released pursuant to this request will not include any information related to testing or treatment I have received for AIDS / HIV unless specifically checked below.

☐ **Release AIDS / HIV related information**

Purpose of disclosure of information:

☐ *Single consent for all future uses and disclosures for treatment, payment, and health care operations*; **OR**

If release is for a specific circumstance, check all applicable items:

☐ Personal use	☐ Insurance claim(s)	☐ Legal issues	☐ Personal use
☐ Follow-up care/continuity of care	☐ Medical record update	☐ Treatment authorization	☐ Follow-up care/ continuity of care

☐ Other (please specify): _____

Section III: RECIPIENT OF INFORMATION

This information is to be disclosed to (check applicable box and complete information below):

☐ My treating providers, health plans, third-party payers (e.g., insurance), accountable care organizations (ACOs), and people helping to operate this program; **OR**

If release is for a specific circumstance, check all applicable items:

☐ Emergency contact	☐ Legal	☐ Treatment provider

THE WRIGHT CENTER FOR COMMUNITY HEALTH

Pt Name _____

DOB _____

MR # _____

Patient ID

☐ Insurance company / managed care organization ☐ Referral source/employee assistance program ☐ Primary care physician office

☐ Laboratory ☐ Pharmacy

☐ Other (please specify): _____

Name of Person or Institution: _____

Address: _____

City/State/Zip Code: _____

Email address: _____ Phone: _____

Fax: _____

Preferred Delivery Method:

☐ Hard Copy Pick Up ☐ Telephone ☐ Fax (for emergent purposes only)

☐ Hard Copy Mail Delivery ☐ Secure Email Transfer ☐ Face-to-face/Verbal exchange

☐ TWC Patient Portal ☐ Third Party Portal _____ (Must Specify a URL Address) ☐ USB Flash Drive

Section IV: EFFECTIVE DATE OF AUTHORIZATION AND REVOCATION

This authorization will expire (enter date or specific occupation): _____. The statement "end of the treatment," "none," or similar language is sufficient if the consent is for a use or disclosure for treatment, payment, or health care operations.

Except to the extent that action has already been taken to comply with this request, this authorization may be revoked:

(1) in writing at any time, by writing to: The Wright Center, Att. Director of Clinical Compliance, 501 S. Washington Avenue, Suite 1000, Scranton, PA 18505; or

(2) verbally, by speaking directly with a representative of The Wright Center, 570.343.2383, ext. 1699.

After The Wright Center receives your notice to revoke, it will terminate this authorization form within 5 business days. Prior to such termination, The Wright Center may have shared some or all of your information or otherwise taken action in reliance on this authorization form; neither the organization nor any of its representatives are liable for any release of information during such time.

Section V: PATIENT RIGHTS AND OTHER IMPORTANT INFORMATION

- You do not have to sign this Authorization Form. If you refuse to sign, it will not affect your ability to obtain treatment, or your eligibility for benefits (if applicable). However, your decision to refuse to give or revoke authorization may result in your insurance company not being able to pay for your care, and you may be responsible for payment of your claim.
- You have the right to inspect the material to be released, subject to the limitations imposed by Pennsylvania regulations, 55 Pa. Code Section 5100.33.
- The Wright Center will provide a disclosure statement and a copy of this signed form along with all records it releases. The recipient of records pursuant to this form may be a HIPAA covered entity or business associate that receives records for purposes of treatment, payment, or health care operations, in which case the records released hereby may be redisclosed in accordance with the permissions contained in the HIPAA regulations, except for uses and disclosures for civil, criminal, administrative, and legislative proceedings against you.
- If you checked the box above that this is a single consent for all future uses and disclosures for treatment, payment, and health care operations, then The Wright Center will need to get a subsequent consent before disclosing any substance use disorder

("SUD") counseling notes, which are a defined type of note prepared by a provider documenting or analyzing the contents of conversation during a SUD counseling session and *not* stored with your other SUD treatment records.

- I understand that the records to be disclosed pursuant to this form include records related to testing, diagnosis, and treatment related to, among other things, SUD, which records are specifically protected by federal and state, including Commonwealth, laws and regulations. I acknowledge that I have been notified of my rights pertaining to the confidentiality of such records by receipt of a Patient Notice. I have had the opportunity to review the Patient Notice and have had my questions about the Patient Notice, if any, answered to my satisfaction.
- Once The Wright Center discloses your health information to the recipient, The Wright Center cannot guarantee that the recipient will not re-disclose this information to a third party or as required by law. The third party may not be required to comply with this Authorization Form or applicable law pertaining to the use and disclosure of your health information.
- The Wright Center will notify you of its decision to approve or deny your request to access or obtain a copy of the requested information within 30 days of receiving this request if the information is maintained or accessible on-site or within 60 days if the requested information is not maintained on-site. If The Wright Center is unable to comply with your request within the specified timeframes, it may extend the applicable deadline for up to 30 days by notifying you in writing.
- The Wright Center uses artificial intelligence ("AI") scribe technology. It is a tool that assists us during patient medical encounters by creating clinical notes based on our conversations. The AI tool does not interact with you directly. It listens to the conversations and creates a secure clinical note. Your provider will then review and approve these clinical notes. This tool allows us to focus more on you, the patient, and less on computer documentation. Currently, AI scribe technology only works with English speaking patients. There may be some inconsistencies in translation for those with limited English proficiency. You have the right to opt out of AI scribe technology by communicating your intention to opt out to your provider and your provider will then disable the technology.
- In accordance with federal and Pennsylvania state law, The Wright Center may charge you for obtaining copies of records, except for copies sent directly to a healthcare facility or physician for continuing care purposes. The Wright Center will bill you directly for any charges incurred. An invoice will be mailed to you and payment will be expected prior to the records being copied or released.
- I have the right to elect not to receive any fundraising communications by providing such an election in writing to the address in the header [or to the following email address: _____@thewrightcenter.org].
- You are entitled to receive a copy of this Authorization Form.

Section VI: PATIENT CONSENT

Written Consent to Release of Health Information:

I have read and understand this Authorization Form and the nature of my release of health information, and I authorize The Wright Center to disclose my health information in the manner described above.

_____	_____
Signature of Patient or Authorized Representative	Date
_____	_____
Printed Name of Authorized Representative (if applicable)	Relationship to Patient
_____	_____
Signature of Witness	Date
_____	_____
Printed Name of Witness	Date

[*verbal consent addressed on the next page*]

THE WRIGHT CENTER FOR COMMUNITY HEALTH

Pt Name _____

DOB _____

MR # _____

Patient ID

Verbal Release of Mental Health Information:

Verbal Consent to Release mental health information is acceptable if the patient is physically unable to provide a signature and verbal consent is witnessed by two persons.

We, the undersigned, certify that _____ was physically unable to provide a signature, that he/she understood the nature of this release and freely gave his/her consent.

Signature of Witness	Date	Signature of Witness	Date
Printed Name of Witness		Printed Name of Witness	

A copy of this Authorization Form must be offered to patients when The Wright Center initiates the authorization request, or when the authorization pertains to drug and/or alcohol treatment records.

☐ I would like a copy of this Authorization Form ☐ I would not like a copy of this Authorization Form

For staff use only:

Signature of Staff Member Obtaining/Processing Consent	Date
Printed Name of Staff Member Obtaining/Processing Consent	

THE WRIGHT CENTER FOR COMMUNITY HEALTH

Pt Name _____

DOB _____

MR # _____

Patient ID

INSTRUCTIONS FOR COMPLETING THE AUTHORIZATION FOR DISCLOSURE OF HEALTH INFORMATION FORM

1. Please complete the Authorization for Disclosure of Health Information Form in its entirety. Incomplete forms will be returned to the sender for completion.

2. The patient or legally authorized representative (see #7 below) must sign and date the form. Electronic signatures are permitted to the extent that they are not prohibited by any applicable law. If you would like to use an electronic signature, please contact us and we will confirm whether it is permitted.

3. Please mail the form to The Wright Center, Att. Director of Clinical Compliance, 501 S. Washington Avenue, Suite 1000, Scranton, PA 18505; fax it to 570.[___.____]; or email it to [_____]@thewrightcenter.org.

4. Except for a single consent for all future uses and disclosures for treatment, payment, and health care operations, records will be sent directly to the party listed as the recipient on the Authorization Form.

5. The following is a list of persons authorized to sign the disclosure of health information form:

- Patients who are 18 years of age or older:
  - If the patient is competent, then the patient must sign. No one else is authorized to sign.
  - If the patient is incompetent, then the legal representative must sign and provide appropriate documentation (e.g., a photocopy of power of attorney documents or other legal documents establishing the authority of the legal representative).
- Patients who are 14 to 17 years of age:
  - If the patient received mental health treatment and consented to his/her own treatment, then the patient must sign.
  - If the patient received mental health treatment and the patient's legal guardian consented to the patient's mental health treatment:

- The patient may sign; or
- The legal guardian may sign if he/she is requesting: (a) the release of records to the patient's current mental health treatment provider; (b) the release of records to the patient's primary care provider (as deemed appropriate by patient's current mental health treatment provider); or (c) if the information is necessary for the legal guardian to consent to the patient's mental health treatment.
  - If the patient received drug/alcohol treatment, then the patient must sign.
- Patients who are under 14 years of age:
  - If the patient received mental health treatment, the patient's legal guardian must sign.
  - If the patient received drug/alcohol treatment, then the patient must sign.
- Patients who are deceased:
  - The patient's legal representative must sign and provide appropriate legal proof (e.g., a photocopy of executor documentation).

Please contact The Wright Center, Director of Clinical Compliance at 570.343.2383, ext. 1699 if you have additional questions or need further assistance.

TAB 11

BUSINESS ASSOCIATE and QUALIFIED SERVICE ORGANIZATION AGREEMENT

WHEREAS, Covered Entity and Business Associate are parties to a Services Agreement ("**Agreement**"), pursuant to which Business Associate performs, or assists in the performance of a function or activity which involves the use or disclosure of Protected Health Information ("**PHI**") or provides consulting to or for the Covered Entity where the provision of the service may involve the disclosure of PHI from the Covered Entity. PHI, as defined below, is information that is subject to protection under the privacy regulations ("**Privacy Regulations**") of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("**Original HIPAA**"), as amended by the Health Information Technology for Economic and Clinical Health Act ("**HITECH**", and collectively with Original HIPAA, the "**HIPAA Statute**"), along with regulations promulgated by the Secretary of the Department of Health and Human Services ("**HHS**") under the HIPAA Statute, including the "**Privacy Rule**" (45 CFR Parts 160 and 164, Subparts A and E) and the "**Security Rule**" (45 CFR Part 160 and 164, Subparts A and C), as amended by the "**Omnibus Rule**" (45 CFR Part 160, Subparts A, B, C and D and Part 164, Subparts A and C) (the Privacy Rule, the Security Rule and the Omnibus Rule, collectively the "**HIPAA Rules**"), as well as any other applicable laws concerning the privacy and security of health information. Hereinafter, the HIPAA Rules and the HIPAA Statute may be collectively referred to as "**HIPAA**;"

WHEREAS, Business Associate is providing scribing services to Covered Entity using an information technology platform for or on behalf of Covered Entity; and

WHEREAS, the Privacy and Security Regulations require Business Associate to enter into an agreement containing specific requirements for use or disclosure of PHI; and

WHEREAS, Covered Entity operates a federally assisted part 2 program in Pennsylvania that must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 USC §290dd-2 and 42 CFR Part 2 (collectively, "Part 2"); and

WHEREAS, Business Associate is also a Qualified Service Organization ("QSO") under Part 2 and must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information; and

WHEREAS, the Parties desire to set forth the terms and conditions pursuant to which Protected Health Information, provided to Business Associate by Covered Entity will be handled between the themselves and third parties.

NOW, THEREFORE, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

Section 1. **Definitions.** The terms used, but otherwise not defined, in this BAA shall have the same meaning as those terms in the Privacy and Security Regulations.

(a) "**Business Associate**" shall mean { Company Name }.

(b) "**Individual**" shall have the meaning set forth in 45 CFR 160.103, including a person who is the subject of the Protected Health Information, and shall include an individual or entity who qualifies as a personal, legal representative of the person, as the context requires.

(c) "**Covered Entity"** shall mean The Wright Center Medical Group d/b/a The Wright Center For Community Health.

(d) "**Privacy Regulations**" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, Subparts A and E, as may be amended, modified or superseded, from time to time.

(e) "**Security Regulations**" shall mean the Standards for Security of Individually Identifiable Electronic Health Information at 45 CFR Parts 160 and 164, Subparts A, C and E, as may be amended, modified or superseded, from time to time.

(f) "**Protected Health Information**" or "**PHI**" shall have the meaning set forth in 45 CFR 160.103, including any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an Individual (including, without limitation, genetic information pertaining to an Individual); or (ii) the provision of health care to an Individual; or (iii) the past, present or future payment for the provision of health care to an Individual; and (iv) that identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

(g) "**Electronic Protected Health Information**" or "**ePHI**" shall mean PHI transmitted or maintained in electronic media.

(h) "**Electronic Media**" shall mean storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

(i) "**Secretary**" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

(j) "**Unsecured PHI**" shall mean Protected Health Information that is not either encrypted or destroyed in accordance with standards set forth in regulations released by the federal Department of Health and Human Services, as the same may be amended from time-to-time.

(k) "Qualified Service Organization" shall have the same meaning as the term "qualified service organization" in 42 CFR §2.11.

Section 2. Obligations of Business Associate.

(a) Permitted Uses. Business Associate shall not use PHI except for the purpose of performing Business Associate's obligations solely in accordance with the Agreement and shall not use PHI in any manner that would constitute a violation of 45 C.F.R. Parts 160 and 164 if so used by Covered Entity.

(b) Permitted Disclosures. Business Associate shall not disclose PHI except for the purpose of performing Business Associate's obligations solely in accordance with the AGREEMENT between the parties and shall not disclose PHI in any manner that would constitute a violation of 45 C.F.R. Parts 160 and 164 if so disclosed by Covered Entity. To the extent that Business Associate discloses PHI to a third party, Business Associate must obtain, prior to making any such disclosure: (i) reasonable assurance from the third party that such PHI will be held in a confidential manner; (ii) reasonable assurance from the third party that such PHI will be used or further disclosed only as required by law or for the purpose

for which it was disclosed to such third party; and (iii) an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of such PHI**,** to the extent the third party has obtained knowledge of such breach. To the extent the Business Associate is to carry out Covered Entity's obligation under 164.504 (e)(2)(ii)(H), Business Associate will comply with the requirements of this subpart that apply to the Covered Entity in the performance of such obligation.

(c) Appropriate Safeguards. Business Associate shall implement appropriate administrative, technical and physical safeguards in compliance with the Privacy Regulations as are necessary to prevent the use or disclosure of PHI, other than as permitted by this BAA/QSOA. To the extent that Business Associate has been engaged to carry out one or more of Covered Entity's obligation(s) under the Privacy Regulations, Business Associate shall comply with the requirements of the Privacy Regulations that apply to Covered Entity in the performance of such obligation(s). Business Associate shall encrypt Covered Entity's PHI when maintained by Business Associate (i.e., "at rest") and when transmitted by Business Associate (i.e., "in transit") to render it unusable, unreadable and/or indecipherable, including any and all of Covered Entity's PHI that Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, transmits or discloses for or on behalf of Covered Entity pursuant to this Agreement. If the Parties otherwise mutually agree that it is not reasonable or possible for Business Associate to encrypt Covered Entity's PHI, then Business Associate shall implement reasonable alternative security methods, as agreed to by Covered Entity in its sole and unfettered discretion, to safeguard Covered Entity's PHI.

(d) Business Associate's Agents and Subcontractors. To the extent Business Associate uses one or more subcontractors or agents to provide services to Covered Entity pursuant to the AGREEMENT and such subcontractors or agents receive or have access to PHI, Business Associate shall require that each subcontractor or agent execute a Subcontractor Agreement as described below; in no event shall any subcontractor of Business Associate be bound to terms less restrictive than this BAA regarding the use, disclosure and protection of PHI and ePHI, and any such subcontractors shall be bound by portions of this BAA regarding breaches of Unsecured PHI and notifications relating to such breaches, which shall be set forth in any agreement between Business Associate and any of its subcontractor(s). Business Associate shall implement and maintain sanctions against subcontractors and agents that violate such restrictions and conditions and shall mitigate the effects of any such violation.

Business Associate shall not transmit Covered Entity's PHI to any Subcontractor or prospective Subcontractor except as otherwise provided herein. In accordance with the Omnibus Rule, Business Associate shall enter into a written subcontractor agreement (the "**Subcontractor Agreement**") with any Subcontractor that creates, receives, maintains, or transmits Covered Entity's PHI on behalf of Business Associate. In the event that Business Associate knows of a pattern of activity or practice of a Subcontractor that constitutes a material breach or violation of the Subcontractor's obligation under the Subcontractor Agreement or other arrangements, Business Associate shall take reasonable steps to cure such breach or end the violation, as applicable, and, if such steps shall be unsuccessful, terminate the Subcontractor Agreement or other arrangements, if feasible. A Subcontractor Agreement shall contain, among other things, the following:

1. The agreement of Subcontractor to comply as to Covered Entity's PHI with the same restrictions and conditions that apply to Business Associate under this Agreement;

2. Subcontractor shall, in accordance with HIPAA, use and disclose only the minimum amount of Covered Entity's PHI necessary for Subcontractor to perform its services under its agreement with Business Associate;

3. Subcontractor shall abide by all Minimum Necessary standards when using and disclosing Covered Entity's PHI;

4. If Subcontractor is an agent of Business Associate, Subcontractor shall not transmit Covered Entity's PHI to any third party or prospective Subcontractor without the prior review or approval by Business Associate of such third party or prospective Subcontractor and/or as otherwise provided in the Subcontractor Agreement;

5. Subcontractor shall use or disclose Covered Entity's PHI only as permitted or required by the Subcontractor Agreement or as required by law;

6. Subcontractor shall not use or disclose Covered Entity's PHI in a manner that would violate the requirements of HIPAA or the Omnibus Rule if done by Covered Entity; and

7. Covered Entity shall be expressly included as a third-party beneficiary to the Subcontractor Agreement and shall be afforded, without limitation, all rights and benefits associated therewith.

(e) Access to PHI. Within five (5) days of receipt of a request from Covered Entity, Business Associate shall make PHI available to Covered Entity for inspection and copying to enable Covered Entity to fulfill its obligations under 45 CFR 164.524. Further, Business Associate shall provide access to PHI as directed by Covered Entity, to an Individual in order to satisfy requirements under 45 CFR 164.524.

(f) Amendment of PHI. Within five (5) days of receipt of a request from Covered Entity, Business Associate shall amend PHI as directed by Covered Entity to enable Covered Entity to fulfill its obligations under 45 CFR 164.526. If a request for amendment of PHI is delivered directly to Business Associate, Business Associate shall, as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity.

(g) Accounting of Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528. Within five (5) days of receipt or a request from Covered Entity, Business Associate shall make available to Covered Entity the information required to provide an accounting of such disclosures. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request (except for disclosures occurring prior to the Effective Date of the AGREEMENT). At a minimum, such accounting information shall include the information described in 45 CFR 164.528(b), including, without limitation: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the written request for disclosure. If a request for an accounting is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity.

(h) Governmental Access to Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI, available to the Secretary in a time and manner designated by Covered Entity or the Secretary, for the purpose of the Secretary determining Covered Entity's compliance with the Privacy Regulations. Business Associate shall provide Covered

Entity access to or a copy of any PHI or other information that Business Associate makes available to the Secretary.

(i) Minimum Necessary Use and Disclosure Requirement. Business Associate shall only request, use and disclose the minimum amount of PHI necessary to reasonably accomplish the purpose of the request, use or disclosure in accordance with 45 CFR 164.502(b). Further, Business Associate will restrict access to PHI to those employees of Business Associate or other workforce members under the control of Business Associate who are actively and directly participating in providing goods and/or services pursuant to the AGREEMENT of the parties and who need to know such information in order to fulfill such responsibilities.

(j) Indemnification. Business Associate shall bear all of Covered Entity's costs, damages, attorney's and consultant's fees, judgments, settlements, and all other associated losses, of any Breach and resultant notifications, if applicable, when the Breach arises from Covered Entity's use of Business Associate's Services, or from Business Associate's negligence, willful misconduct, violation of law, violation of the AGREEMENT, or violation of this Agreement.

(k) Notification of Breach and Mitigation. During the term of this BAA/QSOA, Business Associate shall notify Covered Entity within twenty-four (24) hours of any actual or suspected use and/or disclosure of PHI in violation of the Privacy Regulations or this BAA. Business Associate shall take prompt corrective action to mitigate and cure any harmful effect that is known to Business Associate of an improper use and/or disclosure of PHI in accordance with 45 C.F.R. §164.402, any acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach. For purposes of this BAA/QSOA, a Breach shall be deemed "discovered" by Business Associate as of the first day on which such Breach is actually known to any person, other than the individual committing the Breach, that is an employee, officer, or other agent of Business Associate, or if such Breach should reasonably have been known to Business Associate to have occurred, including but not limited to notification provided to Business Associate by a subcontractor of a Breach. Business Associate shall take all commercially reasonable steps (e.g., audits; hotlines; technological tools, etc.) to allow it to discover Breaches of Security.

(l) Restriction Agreements and Confidential Communications. Business Associate will comply with any agreement that Covered Entity makes that either (i) restricts use or disclosure of Covered Entity's Protected Health Information, or (ii) requires confidential or alternate methods of communication about Covered Entity's Protected Health Information, provided that Covered Entity notifies Business Associate in writing of the restriction or confidential or alternate communication obligations that Covered Entity must follow. Covered Entity will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential or alternate communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement.

(m) Privacy/Security Breach Reporting and Investigations. In the event of a possible Breach of Unsecured PHI, Business Associate shall:

1. promptly and thoroughly investigate any suspected Breach of Covered Entity's Unsecured Protected Health Information not permitted by this Agreement or applicable law;

2. notify Covered Entity regarding a Breach of Covered Entity's Unsecured Protected Health Information ("Covered Entity Privacy Event") without unreasonable delay, but in no event later than five (5) business days of discovering that a Breach occurred, regardless if such Covered Entity Privacy Event is discovered by Business Associate or by any Subcontractor of

Business Associate. Additionally, Business Associate will use its best efforts to assist with Covered Entity's breach investigation by making a timely written report to Covered Entity on any substantiated investigation of a Covered Entity Privacy Event. Business Associate will include as much of the information described in subsection 3) below as is available at the time the report is written and will supplement the report with additional information once that information is known;

3. Business Associate's initial written report concerning a Covered Entity Privacy Event will, at a minimum:

i. identify the names and respective titles of those who conducted the investigation on the part of Business Associate, be delivered on Business Associate's official letterhead, be signed by an officer or director of Business Associate or other responsible person and contain appropriate contact information should Covered Entity need further clarification regarding the content of the report;
ii. identify Covered Entity's Protected Health Information (at the individual level) that was subject to the Breach and the date the Breach occurred;
iii. identify the date the Breach was discovered by Business Associate;
iv. identify the storage medium (e.g. floppy disc, paper record, electronic server) wherein the affected Protected Health Information was housed;
v. identify who committed the Breach of Covered Entity's Protected Health Information and if a disclosure of Covered Entity's Protected Health Information was made, the identity of the person or entity to which that disclosure was made and the date or dates those disclosures occurred;
vi. identify what corrective action Business Associate took or will take to prevent further non-permitted uses or disclosures;
vii. identify what Business Associate did or will do to mitigate any harmful effect of the non permitted use or disclosure; and
viii. provide any other information to Covered Entity as Covered Entity may request to fulfill its reporting obligations to an affected individual as required under 45 C.F.R. §164.410;

4. Business Associate shall assist in and assume all costs of Covered Entity's breach analysis process, including risk assessment, if requested by Covered Entity.

(n) If, following such notification, Business Associate learns additional details about the potential Breach, Business Associate shall notify Covered Entity promptly as such information becomes available. Covered Entity shall determine, in its sole discretion, whether Business Associate or Covered Entity will be responsible for providing notification of any Breach to affected Individuals, the media, the Secretary, and/or any other parties required to be notified under the HIPAA Privacy and Security Rules or other applicable law, unless required otherwise by applicable law. If Covered Entity determines that Business Associate will be responsible for providing such notification, Business Associate may not carry out notification until Covered Entity approves the proposed notices in writing.

(o) To the extent Business Associate is to carry out additional obligations of Covered Entity under the Privacy Rule, Business Associate will comply with the requirements applicable to those obligations.

Section 3. Qualified Service Organization Agreement

(a) Covered Entity and Business Associate hereby agree that this Agreement constitutes a Qualified Service Organization Agreement ("QSOA") as required by 42 CFR Part 2. Accordingly, Business Associate acknowledges that in receiving, storing, processing or otherwise dealing with any Protected Health Information ("PHI", as defined at 45 CFR 160.103) from Covered Entity as a program under 42 CFR Part 2, it is fully bound by said regulations. Further, PHI obtained by Business Associate relating to patients who may have been diagnosed as needing, or who have received, substance use disorder treatment services shall be maintained and used only for the following specific purposes:

(b) In providing the above services as described herein and in the Agreement, Business Associate will conform and comply with all applicable provisions of 42 USC §290dd-2 and the underlying federal regulations, 42 CFR Part 2. This includes but is not limited to resisting any efforts in judicial proceedings to obtain access to the Protected Health Information that is not permitted by the Final Rule modifying the Confidentiality of Substance Use Disorder (SUD) Patient Records and regulations at 42 CFR part 2 ("Part 2")(89 FR 12472, Pgs. 12472-12631). Accordingly, except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity provided that such use or disclosure would not violate the Confidentiality or Privacy Rules if done by Covered Entity.

Section 4. Security of Electronic Protected Health Information (ePHI).

(a) Security. Business Associate will develop, implement, maintain and use appropriate administrative, technical and physical safeguards in compliance with Social Security Act §1173(d) (42 U.S.C. § 1320d-2(d)), 45 C.F.R. Part 164, Subpart C, 45 C.F.R. § 164.530(c), and any other applicable implementing regulations issued by the U.S. Department of Health and Human Services to preserve the availability, integrity, and confidentiality of and to prevent non-permitted use or disclosure of Electronic Protected Health Information ("**ePHI**") created or received for or from Covered Entity. Business Associate will document and keep these safeguards current.

(b) Agents and Subcontractors. Business Associate will ensure that any agent, including a subcontractor, to whom it provides ePHI agrees to implement security safeguards described in subsection (a) of this Section, and that such subcontractors are bound by the terms and conditions of subsection (d) of Section 2 and this Section 4.

(c) Security Incidents. Business Associate will, within twenty-four (24) hours, report to Covered Entity any security incident of which it becomes aware. This includes, but is not limited to attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations.

Section 5. Term and Termination.

(a) Term. This BAA/QSOA shall commence on the Effective Date of the AGREEMENT and will remain effective for the entire term of the AGREEMENT between the parties, unless earlier terminated in accordance with the terms herein.

(b) Termination of Agreement. This BAA/QSOA will immediately terminate without notice upon termination of the AGREEMENT.

(c) For Cause Termination Due to Material Breach. In the event of a material breach by Business Associate of any of its obligations hereunder, Covered Entity shall have the right, as

specifically recognized by Business Associate, to terminate this BAA/QSOA and the AGREEMENT between the parties, at any time by providing Business Associate written notice of termination setting forth a description of the breach and the effective date of termination.

(d) Effect of Termination. As of the effective date of termination of this BAA/QSOA, neither party shall have any further rights or obligations hereunder except: (a) as otherwise provided herein or in the AGREEMENT between the parties; (b) for continuing rights and obligations accruing under the Privacy Regulations; or (c) arising as a result of any breach of this BAA/QSOA, including, but not limited to, any rights and remedies available at law or equity. Upon termination of this BAA/QSOA for any reason, Business Associate shall return or destroy all PHI (regardless of form or medium), including all copies thereof and any data compilations derived from PHI and allowing identification of any Individual who is the subject of PHI, except as otherwise required by law. The obligation to return or destroy all PHI shall also apply to PHI that is in the possession of agents or subcontractors of Business Associate. If the return or destruction of PHI is not feasible, Business Associate shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon mutual agreement of the parties that return or destruction of PHI is not feasible, Business Associate shall continue to extend the protections of this BAA to such information, and limit further uses or disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible, for as long as Business Associate maintains such PHI. If Business Associate elects to destroy the PHI, Business Associate shall notify Covered Entity in writing that such PHI has been destroyed. Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) days following the effective date of the termination or other conclusion of the Agreement.

Section 6. Miscellaneous.

(a) Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of HIPAA and any other applicable law.

(b) Conflicts. The terms and conditions of this BAA/QSOA will override and control any conflicting term or condition of the Agreement. All non-conflicting terms and conditions of the services agreement remain in full force and effect.

FOR:	**FOR:**
[Name of Company]	**The Wright Center for Community Health**
_____	_____
[name], Authorized Signatory	{ TWCCH Signatory }
Date: _____	Date: _____

INSURANCE REQUIREMENTS

The Parties shall carry and at all times maintain in full force and effect, at its sole expense, policies of products/completed operations liability, errors and omissions, comprehensive general liability, cyber liability (including, but not limited to, data breaches) and professional liability insurance from an insurance company authorized to do business in the Commonwealth of Pennsylvania or which holds a Pennsylvania Certificate of Authority, in the minimum amounts set forth below for each policy year to insure TWCCH and its officers, directors, trustees, employees and agents against any claim or claims for damages arising by reason of personal injuries or death occasioned, directly or indirectly, and for any other claim or claims for damages due to the acts or omissions of the other party in connection with the performance of its obligations under this Agreement. This insurance shall be issued to the other Party as a named insured and shall contain an express requirement that each Party shall receive written notice from the insurer at least thirty (30) days prior to any cancellation, reduction or non-renewal of any such insurance coverage. Memorandum copies of the above insurance policies shall be provided to TWCCH upon its request.

[VENDOR] shall obtain and maintain insurance of the types and in the amounts described below:

TYPE OF COVERAGE	[VENDOR]**: Minimum AMOUNT OF COVERAGE**	**TWCCH: Minimum AMOUNT OF COVERAGE**
AD.1 Worker's Compensation Employer's Liability	Statutory limits $1 million Employer's liability	Statutory limits $1 million Employer's liability
AD.2 Commercial General Liability: this shall cover liability arising from premises, operations, independent contractors, products-completed operations, personal injury and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).	$2 million per occurrence/$2 million aggregate	$2 million per occurrence/$2 million aggregate
AD.3 Business Auto Liability: covering any automobile, including hired and non-owned autos.	$1 million per occurrence/$1 million aggregate	$1 million per occurrence/$1 million aggregate
AD.4 Professional Liability Insurance Policy: covering all errors and omissions liability appropriate for the services provided by [VENDOR] with respect to services rendered under this Contract with no more than a	$1 million per occurrence/$3 million aggregate	$1 million per occurrence/$3 million aggregate

$50,000 per occurrence deductible to be borne by [VENDOR]		
AD.5. Cyber Liability and Data Breach	$20 million per occurrence/$20 aggregate	$5 million per occurrence/$5 million aggregate

TAB 12

Notification to Secretary of Health and Human Services of

Unsecured Protected Health Information Breach

As a covered entity The Wright Center for Community Health (TWCCH) must notify the Secretary of Health and Human Services if it discovers a breach of unsecured protected health information. See 45 C.F.R. § 164.408. All notifications must be submitted to the Secretary using the Web portal below.

A covered entity's breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate, and, if it discovers additional information, submit updates in the manner specified below. If only one option is available in a particular submission category, the covered entity should pick the best option, and may provide additional details in the free text portion of the submission.

If a covered entity discovers additional information that supplements, modifies, or clarifies a previously submitted notice to the Secretary, it may submit an additional form by checking the appropriate box to indicate that it is an addendum to the initial report, using the transaction number provided after its submission of the initial breach report.

Instructions below for submitting breach notifications.

Breaches Affecting 500 or More Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

Submit a Notice for a Breach Affecting 500 or More Individuals

View a list of Breaches Affecting 500 or More Individuals

Breaches Affecting Fewer than 500 Individuals

If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. The covered entity must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.

Submit a Notice for a Breach Affecting Fewer than 500 Individuals

If you have questions or would like to provide feedback about the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification process, or OCR's investigative process, please send us an email at OCRbreachreportingfeedback@hhs.gov.
Content created by Office for Civil Rights (OCR)

Notification to Secretary of Health and Human Services of Unsecured Protected Health Information Breach

For Use if Electronic Means of Reporting are Unavailable

This form in not in the Electronic Health Record

Date: _____/_____/20_____

Dear Secretary of the Department of Health and Human Services (HHS):

The purpose of this notification is to inform you that our organization has experienced a breach of security that has resulted in the compromise of the confidential protected health information of five hundred (500) or more individuals. This notification is provided to you in accordance with regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

1. Brief description of the breach event: **[include date of breach and date of discovery, number of affected individuals]**

_____
_____
_____

2. Description of types of information involved in the breach: **[i.e., name, SSN, DOB, address, etc.]**

_____
_____
_____

3. We are asking affected individuals to take the following steps to protect themselves from potential harm resulting from the breach:

_____
_____
_____

4. We are taking the following steps to investigate the breach and its causes, to mitigate losses and to protect against further breaches:

_____
_____
_____

5. Should you have any questions about the breach or any information contained in this notification, please contact our Privacy Officer as follows:

Phone – 570.343.2353 x1699

Email – twc-hipaa@thewrightcenter.org

Sincerely,

_____
[Printed Name, Title]

THE WRIGHT CENTER for COMMUNITY HEALTH

Notification to Media Outlets of Unsecured Protected Health Information Breach

Dear: _____ Date: _____/_____/20_____

The purpose of this notification is to inform you that our organization has experienced a breach of security that has resulted in the compromise of the confidential protected health information of five hundred (500) or more patients. This notification is provided to you in accordance with regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its purpose is to provide you with the information you need to accurately report this breach to local patients so that they are informed and can appropriately respond to the breach.

1. Brief description of the breach event: **[include date of breach and date of discovery]**

_____
_____
_____
_____

2. Description of types of patient information involved in the breach: **[i.e., name, SSN, DOB, address, etc.]**

_____
_____
_____
_____

3. We are asking patients to take the following steps to protect themselves from potential harm resulting from the breach:

_____
_____
_____
_____

4. We are taking the following steps to investigate the breach and its causes, to mitigate losses and to protect against further breaches:

_____
_____
_____
_____

5. Should you have any questions about the breach or any information contained in this notification, please contact our Privacy Officer as follows:

Phone – 570.343.2353 x1699

Email – twc-hipaa@thewrightcenter.org

Sincerely,

_____
[Printed Name, Title]

This document is not part of the patient's electronic health record.

Revised: January 17, 2025

TAB 13

EMPLOYEE CONFIDENTIALITY AGREEMENT REGARDING PROTECTED HEALTH INFORMATION (PHI)

This Confidentiality Agreement Regarding Protected Health Information (PHI) (the "Agreement") is made and entered into as of [Date] (the "Effective Date"), by and between [Company Name], a company organized and existing under the laws of [State/Country], with its principal place of business at [Company Address] ("Company"), and [Employee Name], residing at [Employee Address] ("Employee").

WHEREAS, Employee is employed by Company; and

WHEREAS, during the course of Employee's employment, Employee may have access to Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations;

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the parties agree as follows:

1. **Definition of PHI.** "Protected Health Information" or "PHI" means individually identifiable health information, including demographic data, that is:

    * Created or received by a health care provider, health plan, employer, or health care clearinghouse; and
    * Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

2. **Obligations of Employee.** Employee agrees to the following with respect to PHI:

    * To keep all PHI strictly confidential and not disclose it to any unauthorized third party.
    * To use PHI solely for the purpose of performing Employee's duties for Company, and only to the extent necessary to perform those duties.
    * To comply with all applicable provisions of HIPAA and Company's policies and procedures regarding the privacy and security of PHI.
    * Not to access, use, or disclose PHI for any purpose other than those permitted by Company and HIPAA.
    * To report immediately to Company any suspected or actual unauthorized access, use, or disclosure of PHI.
    * To protect PHI with appropriate safeguards, including physical, technical, and administrative safeguards, to prevent unauthorized access, use, or disclosure.
    * Upon termination of Employee's employment, to return all PHI, whether in electronic or physical form, to Company or destroy it as directed by Company.

3. **Permitted Uses and Disclosures.** Employee understands that PHI may only be used or disclosed as permitted by HIPAA and Company policy, which may include:

* For treatment, payment, and health care operations;
* With authorization from the individual;
* As required by law; or
* For other specific purposes permitted by HIPAA.

4. **Business Associate Agreement (if applicable).** If Employee's work involves a Business Associate Agreement (BAA) between Company and another entity, Employee agrees to comply with the terms and conditions of the BAA.

5. **Training.** Employee acknowledges receipt of training on HIPAA and Company's privacy and security policies and procedures.

6. **Disciplinary Action.** Employee understands that failure to comply with this Agreement or HIPAA may result in disciplinary action, up to and including termination of employment.

7. **Term.** This Agreement shall remain in effect during the term of Employee's employment with Company and shall continue to be binding upon Employee after the termination of Employee's employment, without limitation in time.

8. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of [State].

9. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous communications and proposals, whether oral or written.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

_____
[Company Name]

By: _____
Name: [Name of Authorized Signatory]
Title: [Title of Authorized Signatory]

_____
[Employee Name]

Key Points and Legal Disclaimer:

- **This is a SAMPLE agreement only and should NOT be used without the advice of experienced legal counsel specializing in HIPAA compliance.** HIPAA regulations are complex and subject to change.
- **This agreement must be tailored to your specific organization's policies and procedures.**
- **You MUST have a Business Associate Agreement (BAA) in place with any vendors or subcontractors who will have access to PHI.** This agreement outlines the responsibilities of the business associate regarding the protection of PHI.
- **Regular HIPAA training for all employees is essential.** This agreement should be part of a broader HIPAA compliance program.
- **State laws may provide additional privacy protections beyond HIPAA.** Your legal counsel can advise you on these requirements.

This example provides a starting point. **Do not use it without consulting with an attorney specializing in healthcare privacy law.** Using a generic template without legal review can create significant legal risks.