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): • Audit Committee • TWCCH Board	*Date Policy Originally Established:* August 30, 2019 Revised: April 24, 2020; October 2025; April 27, 2026; November 17, 2026 Reviewed: September 18, 2024
Date(s) of Last Approval: Committee Approval: October 18, 2024 Board Approval: October 25, 2024 | October 31, 2025 | May 29, 2026 | November 20, 2026	*Next Review Date:* May 2027

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.

GUIDELINES/DEFINITIONS

- 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.
- All employees providing healthcare and related services for or on behalf of Provider's patients, also known as "authorized personnel."
- "Treatment" means the provision, coordination, or management of healthcare and related services by one or more health care providers.
- "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.
- "Health Care Operations" means certain operational and administrative tasks undertaken by a health care provider or health plan, including such things as
    - quality assessment and quality improvement;
    - reviewing and evaluating the competence or qualifications of health care professionals;
    - contract placement, including underwriting, premium rating and other activities relating to the creation, renewal or replacement of a health insurance or health benefits contract;
    - arranging for certain professional services such as legal or audit review services;
    - business planning and development;
    - resolution or internal grievances; and
    - customer service activities.
- 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 ("DHHS").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.

I. 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 above) and to perform certain "health care operations" (as that term is defined above) necessary for the proper functioning of WCMG.
    1. No employee, contracted employee, or learner shall access, view, modify, or disclose an Electronic Health Record (EHR) or Protected Health Information (PHI) without a legitimate, direct business, or clinical need required to fulfill their assigned job duties.
    2. Employees, contracted employees, and learners are strictly prohibited from using their professional access credentials to access, view, modify, or search for their own health records/EHR, as well as the medical records of family members, relatives, friends, co-workers, or any other personal acquaintances, regardless of whether verbal or written authorization or consent has been granted. Access to one's own personal health records or those of personal relations must occur through standard patient medical records release of records request procedures or via the patient portal. All EHR activities are logged and monitored; failure to adhere to this policy constitutes a HIPAA security violation subject to immediate disciplinary action, up to and including termination.

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 the Provider or any of its Authorized Personnel sell PHI in exchange for any form of remuneration of any kind.

II. 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.

III. 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.

IV. 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

V. 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, the 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. The 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, the 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. The 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.

VI. Policy on Authorizations

A. For all uses and disclosures of PHI that are not described in Section III 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. See (Confidentiality of Substance Use Disorder Patient Records, 2024) or (42 C.F.R. § 2, 2024).

VII. 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.

VIII. 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.

IX. 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.

X. 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.

XI. 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.

XII. 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.

XIII. 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, Senior Cyber & HIPAA Security Administrator and other IT personnel, as needed (collectively, the "Security Team").

Areas reviewed by the Senior Cyber & HIPAA Security Administrator 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 Senior Cyber & HIPAA Security Administrator 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.

The Senior Cyber & HIPAA Security Administrator (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.

The provider then ranks the level of risk remaining after considering existing risk management factors. From this assessment, the 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. Senior Cyber & HIPAA Security Administrator 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 the 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 Senior Cyber & HIPAA Security Administrator, 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 R and 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 Provider's 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)
12§164.312(a)https://docs.google.com/document/d/1kXmzcpWIg2nZwn6Ut9l4jtcuGrbrMmrV/edit?usp=sharing&ouid=109473183898298177643&rtpof=true&sd=true
13 §164.312(b)
14 §164.312(c)(1)
15 §164.312(d)
16 §164.314(a)(1)
17 (Confidentiality of Substance Use Disorder Patient Records, 2024) or (42 C.F.R. § 2, 2024)

REFERENCE

eCFR :: 45 CFR Part 164 -- Security and Privacy
https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2
EOS© Toolbox

Helayna Szescila

Helayna Szescila
Deputy Chief Governance Officer & Assistant Secretary