THE WRIGHT CENTER for COMMUNITY HEALTH

THE WRIGHT CENTER FOR COMMUNITY HEALTH ("TWCCH")

HIPAA COMPLIANCE BINDER

THE WRIGHT CENTER FOR COMMUNITY HEALTH
HIPAA COMPLIANCE BINDER

TABLE OF CONTENTS

TAB

CONFIDENTIALITY OF MEDICAL/HEALTH INFORMATION POLICIES & PROCEDURES

TABLE OF CONTENTS

TAB 1

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Confidentiality of Medical/Health Information Policies and Procedures

I. Policy Statement and Purpose

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.

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.

II. Definitions.

(a) 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.

(b) All employees providing healthcare and related services for or on behalf of Provider's patients, also known as "authorized personnel."

(c) "Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers.

(d) "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.

(e) "Health Care Operations" means certain operational and administrative tasks undertaken by a health care provider or health plan, including such things as (1) quality assessment and quality improvement; (2) reviewing and evaluating the competence or qualifications of health care professionals; (3) contract placement, including underwriting, premium rating and other activities relating to the creation, renewal or replacement of a health insurance or health benefits contract; (4) arranging for certain professional services such as legal or audit review services; (5) business planning and development; (6) resolution or internal grievances; and (7) customer service activities.

III. Protection of PHI

A. Only the following representatives of the Provider are entitled to have access to PHI:

- 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 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 TWCCH 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 **TWCCH**.

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 not be left lying in areas where unauthorized persons may view or otherwise access it. Any paper PHI should be uploaded into the EMR and then destroyed.

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.

According to 45 CFR 164.408:

(a) ***Standard.*** A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) ***Implementation specifications: Breaches involving 500 or more individuals.*** For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.

(c) ***Implementation specifications: Breaches involving less than 500 individuals***. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the matter specified on the HHS web site.

IV. Uses and Disclosures for which No Authorization Required.

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

1. Policy. It is the 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.

B. 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:

- public health purposes;
- health oversight activities;
- judicial and administrative proceedings;

- law enforcement;
- disclosures to personal representatives;
- disclosures to family members involved in an individual's care;
- to avoid serious threats to health and safety;
- for workers' compensation functions;
- to protect victims of abuse, neglect or domestic violence; and
- to effect 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 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, 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. Provider will make sure that the notice is available for individuals visiting Provider for services, in the event that they ask for a copy.

6. 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 <u>not</u> 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; <u>provided</u> 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:

(i) the individual's request for an amendment;

(ii) the denial of the request;

(iii) the individual's statement of disagreement, if any; and

(iv) 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 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 an adequate accounting. The HIPAA Compliance Officer shall respond to a request for an accounting of disclosures by providing the individual with copies of all 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

1. 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.

2. 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

1. 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.

2. 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.

3. 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

1. 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.

2. Procedures.

(a) 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.

(b) The Provider, after determining what steps can mitigate the harmful effect, shall determine which of these steps is most practicable, and take such actions.

(c) 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, 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.

XVI. 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 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. Provider 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.

[1] §164.308(a)(1)(i)

4. **Information System Activity Review**. 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:

- the development and implementation of security measures to protect ePHI, and
- 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:

- All employees providing healthcare and related services for or on behalf of Provider's patients, also known as authorized personnel.

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.

---

[2] §164.308(a)(2)
[3] §164.308(a)(3)(i)
[4] §164.308(a)(4)
[5] §164.308(a)(5)(i)

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 R and the Privacy Policies.

---

[6] §164.308(a)(6)(i)
[7] §164.308(a)(7)(i)
[8] §164.308(a)(8)

K. Facility Access Controls (Physical Safeguard).[9] Provider limits physical access to electronic information systems and the facility in which they are housed, and ensure 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.

Provider has developed a contingency that plan 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.

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 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 re-using or replacing the media.

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 e-mails 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 e-mail 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.

---

[9] §164.310(a)(1)
[10] §164.310(b)
[11] §164.310(d)(1)
[12] §164.312(a)

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 Provider.
- 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.

---

[13] §164.312(b)
[14] §164.312(c)(1)
[15] §164.312(d)
[16] §164.314 (a)(1)

TAB 2

Date: _____

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 will disclose only the Minimum Necessary of PHI.

---

1. **Name of person requesting information:** _____

2. **Check if requesting in capacity as individual:** _____ (If not checked, go to #3)

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

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

   - **Check if individual's identity verified by photo I.D.** _____ (attach copy of I.D.)

   - **Attach all documents provided to support person's authority to access 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 Compliance Official 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 person's authority to act on behalf of entity:**

     - o _____ Agency identification badge
     - o _____ Statement on government letterhead
     - o _____ Statement on organization letterhead (if not government agency)
     - o _____ Other (specify: _____)

   - **Check if individual's identity verified by photo I.D.** _____ (attach 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 entity's authority to access PHI requested**
- **If unable to verify the requesting person's identity and/or the authority of his or her entity 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 HIPAA Compliance Officer immediately.**
- **Employee comments:**
  _____
  _____

Employee Name (Printed): _____

Employee Signature: _____ Date: _____

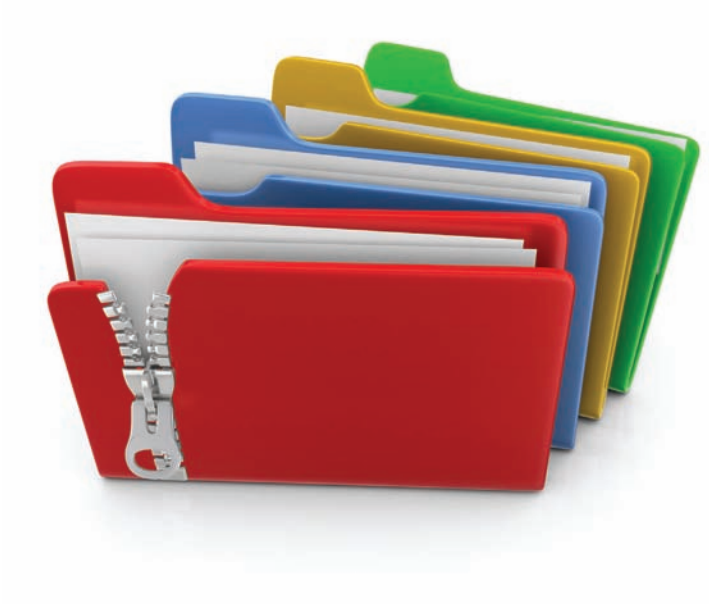
Check if reviewed by HIPAA Compliance Officer: _____

HIPAA Compliance Officer Signature: _____ Date: _____

TAB 3A

THE WRIGHT CENTER for COMMUNITY HEALTH

501 South Washington Avenue, Suite 1000
Scranton, PA 18505
www.thewrightcenter.org
David Beecham, Compliance Officer
Office Phone: (570) 343-2383 x 1032



Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

Please review it carefully.

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record	• You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this. • We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.
Ask us to correct your medical record	• You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this. • We may say "no" to your request, but we'll tell you why in writing within 60 days.
Request confidential communications	• You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address. • We will say "yes" to all reasonable requests.

continued on next page

Your Rights *continued*

Ask us to limit what we use or share	• You can ask us **not** to use or share certain health information for treatment, payment, or our operations. • We are not required to agree to your request, and we may say "no" if it would affect your care. • If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. • We will say "yes" unless a law requires us to share that information.
Get a list of those with whom we've shared information	• You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with, and why. • We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.
Get a copy of this privacy notice	• You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.
Choose someone to act for you	• If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. • We will make sure the person has this authority and can act for you before we take any action.
Contact us if you feel we have not honored your privacy rights	• If you believe we have not honored your privacy rights, contact us using the information on page 1. • You may also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints.** • You will not be penalized for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:	• Share information with your family, close friends, or others involved in your care • Share information in a disaster relief situation • Include your information in a hospital directory • Contact you for fundraising efforts *If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.*
In these cases we *never* share your information unless you give us written permission:	• Sale of your information • Most sharing of psychotherapy notes

Our Uses and Disclosures

How do we typically use or share your health information? We typically use or share your health information in the following ways.

Treat you	• We can use your health information and share it with other professionals who are treating you. • We may use and disclose information to contact you as a reminder that you have an appointment. • We may call your name in the waiting room at TWCCH to notify you that the physician, nurse or other professional is ready to see you.	***Example:*** *A doctor treating you for an injury asks another doctor about your overall health condition.*
Run our organization	• We can use and share your health information to run our practice, improve your care,and contact you when necessary.	***Example:*** *We use health information about you to manage your treatment and services.*
Bill for your services	• We can use and share your health information to bill and get payment from health plans or other entities.	***Example:*** *We give information about you to your health insurance plan so it will pay for your services .*

continued on next page

How else can we use or share your health information?

We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.**

Unless you object, we may release information about you to a friend or family member who is involved in your medical care. We may also give information to someone who helps pay for your care. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status, and location.

Help with public health and safety issues	• We can share health information about you for certain situations such as: • Preventing disease • Helping with product recalls • Reporting adverse reactions to medications • Reporting suspected abuse, neglect, or domestic violence • Preventing or reducing a serious threat to anyone's health or safety
Do research	• We can use or share your information for health research.
Service Excellence	• We will follow up your visit with us with an electronic survey. Please take a few minutes to let us know about your satisfaction with your visit.
Comply with the Law	• We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.
Respond to organ and tissue donation requests	• We can share health information about you with organ procurement organizations.
Work with a medical examiner or funeral director	• We can share health information with a coroner, medical examiner, or funeral director when an individual dies
Address workers' compensation, law enforcement, and other government requests	• We can use or share health information about you: • For workers' compensation claims • For law enforcement purposes or with a law enforcement official • With health oversight agencies for activities authorized by law • For special government functions such as military, national security, and presidential protective services
Respond to lawsuits and legal actions	• We can share health information about you in response to a court or administrative order, or in response to a subpoena.
Military and Veterans	• If you are a member of the armed forces, we may release information about you as required by military authorities. We may also release information about foreign military personnel to the appropriate foreign military authority.
National Security and Intelligence Activities	• We may release information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.**

Changes to the Terms of This Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

This Notice of Privacy Practices applies to the following organizations: The Wright Center for Community Health

Effective11/2018

David Beecham, Compliance Officer
Office Phone: (570) 343-2383 x 1032
Email: hipaa@thewrightcenter.org

TAB 3B

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Acknowledgement of Receipt of Notice of Privacy Practices

Patient Name & Address: _____

_____

_____

I have received a copy of the Notice of Privacy Practices for the above named practice.

_____ _____

Signature Date

For Office Use Only

We were unable to obtain a written acknowledgement of receipt of the Notice of Privacy Practices because:

- ☐ **An emergency existed & a signature was not possible at the time.**
- ☐ **The individual refused to sign.**
- ☐ **A copy was mailed with a request for a signature by return mail.**
- ☐ **Unable to communicate with the patient for the following reason:**_____

_____

- ☐ **Other:**

_____

_____

Signature: _____

Date: _____ _____

Eff. 11/2018

TAB 4

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 that 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 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:

- Where 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's Name	Patient's Signature	Date
_____	_____	_____
Received by Employee (print name)	Employee Signature	Date

Employees must transmit this completed form to the HIPAA Compliance Officer via the Electronic Health Record.

TAB 5

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.

SECTION A: Individual requesting records amendment.

Name: _____

Address: _____

Telephone: _____ E-mail: _____

Date of Birth: _____

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: _____

Eff. 11/2018

TAB 6

THE WRIGHT CENTER FOR COMMUNITY HEALTH
Individual Request for an Accounting of Disclosures
Protected Health Information

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: _____

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: _____

Eff. 11/2018

TAB 7

THE WRIGHT CENTER **FOR COMMUNITY HEALTH**

Patient Authorization to Release/Obtain Protected Health Information

Patient Information:

Name	Date of Birth	Patient Account #
Address		Telephone

I authorize The Wright Center to release/obtain the information described in this form to:

Name of Provider, Person or Facility to whom information is to be released:	Telephone of Provider, Person or Facility
Address of Provider, Person or Facility	

for the purpose of: ☐ continuation of medical treatment ☐ payment of bill
☐ Worker's Compensation ☐ education ☐ legal purposes ☐ insurance purposes
☐ at the request of the patient or the patient's legal representative for personal access or
☐ other (specify):

_____
_____
_____

The information to be released will cover the time period from _____ to _____

SPECIFIC INFORMATION TO RELEASE/OBTAIN: ☐ **ALL RECORDS**

☐ Clinic Notes (NOT psychotherapy notes)

☐ Discharge Summary	☐ History & Physical	
☐ Medications	☐ X-Ray Reports	☐ Colonoscopy
☐ EEG, EKG, Stress Test	☐ Immunizations	☐ Operation Report(s)
☐ Consultation Report(s)	☐ Emergency Dept. Notes	☐ Itemized Bills
☐ Pathology Reports	☐ Disability/FMLA Form	☐ Endoscopy
☐ Laboratory Reports	☐ X-Ray Films	

☐ Other (specify):

_____
_____

☐ ***Psychotherapy Notes*** (Psychotherapy Notes are recorded by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of your medical record. Psychotherapy Notes include: medication prescription and monitoring, modalities and frequencies of treatment furnished, and results of clinical tests, and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, progress and progress-to-date.) *Disclaimer: The Wright Center reserves the right to refuse to release psychotherapy notes if disclosure is deemed not to be in the best interests of the patient.*

SPECIAL AUTHORIZATION: If you are authorizing The Wright Center to release/obtain information related to the testing, diagnosis and/or treatment for any of the following conditions, please initial in front of the section which describes the type of information to be released:

☐ My evaluation, testing, diagnosis or treatment for *alcoholism and/or drug abuse or dependence* may be released to the recipient noted on the signed authorization.
☐ My evaluation, testing, diagnosis or treatment concerning my *mental health/rehabilitation information* may be released to the recipient noted on the signed authorization.
☐ My testing, diagnosis or treatment for *HIV/AIDS* may be released to the recipient noted on this signed authorization.

I understand that authorizing disclosure of health information is voluntary. I understand that I may inspect or obtain a copy of the information to be disclosed. I understand a fee may be charged for each copy of my medical record, and that health records will be provided in electronic format unless I request hard copies (which will cost an additional fee). I understand The Wright Center will provide me with a copy of the signed authorization form. If I have questions about disclosure of my health information, I can contact The Wright Center's Privacy Officer.

By signing my name to this form, I understand and agree to the following:

Authorization: I certify that this request is made voluntarily and that the information given above is accurate to the best of my knowledge. I understand that if I have authorized the disclosure of my health information to someone who is not legally required to keep it private, it may be re-disclosed and may no longer be protected pursuant to HIPAA regulations/federal law. A copy or fax of this authorization will be as valid as the original.

Cancelling This Authorization: I understand that I may change my mind and cancel this authorization at any time in writing provided to The Wright Center. After The Wright Center receives my written notice, it will cancel this release within five (5) business days. During these five days, The Wright Center may have shared some or all of my information. Neither The Wright Center nor any of its representatives are liable for any release of information during this time.

Right of Refusal: I have the right NOT to sign this authorization. My refusal to sign this form will not affect my/the patient's eligibility for treatment or benefits.

Revocation and Expiration: I understand that this authorization is revocable by me, in writing, at any time, except to the extent that action has been taken in reliance on it. I will contact The Wright Center immediately if I wish to revoke this authorization.

Unless I revoke this authorization in writing, this authorization will expire automatically:

☐ when the records requested on this authorization have been released, or
☐ one year from the date I sign it

The Wright Center may not condition my treatment or payment for my treatment on obtaining this authorization from me, unless this authorization is requested (i) to provide research-related treatment to me, or (ii) because the health care being provided to me is solely for the purpose of creating protected health information for disclosure to a third party.

NOTE: IF PATIENT IS UNDER 14 YEARS OF AGE AND IS NOT AN EMANCIPATED MINOR THE PARENT OR GUARDIAN MUST SIGN.

Date/Time: _____

Patient/Parent or Legal Guardian Signature: _____

If Legal Guardian or Personal Representative, proof of guardianship or Power of Attorney must be attached.

Date/Time: _____

Witness Signature: _____

Verbal Authorization: If patient is unable to sign authorization form because of emergency, physical condition or age, describe the circumstances:

_____
_____
_____ .
_ _____

Signature:_____ Relationship: _____

Witness:_____ Date/Time: _____

****

A COPY OF THE COMPLETED AUTHORIZATION FORM MUST BE GIVEN TO PATIENT/GUARDIAN/ REPRESENTATIVE

☐ As Medical Record Clerk, I have released the Minimum Necessary documentation required according to HIPAA.

Name of Staff Member providing copy to patient/legal guardian or personal representative.

Name: **Date:**

TAB 8

HIPAA BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("BAA") is made and entered into as of this ___ day of by and between **THE WRIGHT CENTER FOR COMMUNITY HEALTH,** its subsidiaries and affiliates (hereinafter collectively referred to as the "Covered Entity") and **"NAME"** ("Business Associate"). This BAA is effective on the effective date of the Consulting Services Agreement between the parties (the "Effective Date").

WHEREAS, Covered Entity and Business Associate are parties to an Agreement for Consulting Services ("Primary Agreement"), pursuant to which Business Associate performs, or assists in the performance of a function or activity which may involve 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, Covered Entity requires that Business Associate protect the privacy and provide for the security of PHI in compliance with the Privacy and Security Regulations; and

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

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) "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.

(b) "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.

(c) "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.

(d) "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.

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

(f) "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.

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

(h) "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.

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 Primary 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 Primary 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.

(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. 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 Primary 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 his/her/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 his/her/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 his/her/its agents or subcontractors for at least six (6) years prior to the request (except for disclosures occurring prior to the Effective Date). 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 his/her/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 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 Primary Agreement of the parties and who need to know such information in order to fulfill such responsibilities.

(j) Notification of Breach. During the term of this BAA, 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, 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.

Section 3. 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 3, and that such subcontractors are bound by the terms and conditions of subsection (d) of this Section 3.

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

(d) Breaches of Unsecured PHI. If Business Associate accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses Unsecured PHI, Business Associate shall, within fifteen (15) days following the discovery of a breach of such information, notify Covered Entity of such breach. Such notice shall include (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during such breach; (ii) a brief description of the event (including the date of the breach and the date of the discovery of the breach, if known; (iii) a description of the types of information involved in the breach; (iv) a brief description of the steps that Business Associate is taking to investigate the breach, to mitigate losses, and to protect against further breaches; and (v) the steps Business Associate thinks individuals should take to protect themselves from potential harm resulting from the breach.

Section 4. Term and Termination.

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

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

(c) For Cause Termination Due to Material Breach. In the event of a material breach by Business Associate of any of his/her/its obligations hereunder, Covered Entity shall have the right, as specifically recognized by Business Associate, to terminate this BAA and the Primary 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, neither party shall have any further rights or obligations hereunder except: (a) as otherwise provided herein or in the Primary 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, including, but not limited to, any rights and remedies available at law or equity. Upon termination of this BAA 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. 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.

Section 5. Indemnification. Business Associate shall indemnify and hold Covered Entity, and its employees, officers, directors, independent contractors, agents and representatives, harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other expenses, of any kind or nature whatsoever, including, without limitation, attorneys' fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach of this BAA by Business Associate. The obligations set forth in this Section 5 shall survive termination of this BAA, regardless of the reasons for termination.

Section 6. Assignment. This BAA and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred by the Business Associate without the prior written consent of the Covered Entity and any assignment or transfer without proper consent shall be null and void.

Section 7. Governing Law and Venue. This BAA shall be governed by, and interpreted in accordance with, the Privacy Regulations and the laws of the Commonwealth of Pennsylvania.

Section 8. Amendment or Modification. This BAA may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event

provisions of this BAA shall conflict with the requirements of the Privacy Regulations, this BAA shall automatically be deemed amended as necessary to comply with such legal requirements.

Section 9. **Waiver.** The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

Section 10. **Severability.** In the event that any provision or part of this BAA is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this BAA, with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

Section 11. **Entire Agreement.** This BAA constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written negotiations, commitments, and understandings relating thereto.

IN WITNESS WHEREOF, Covered Entity and Business Associate have each caused this BAA to be executed in their respective names by their duly authorized representatives, as of the date written herein above.

The Wright Center for Community Health	**Business Associate**
By: _____	By: _____

TAB 9

THE WRIGHT CENTER FOR COMMUNITY HEALTH
EMPLOYEE CONFIDENTIALITY STATEMENT

As an employee of The Wright Center for Community Health ("TWCCH"), I recognize that I may have access to documents and records containing confidential information about patients. I recognize and agree that this confidential patient information must be protected, and that it is my duty as an employee to actively ensure that any confidential information that I handle is protected to the greatest extent possible. As such, I hereby agree to adhere to the following guidelines in order to ensure that confidential patient information is handled with care and in a manner consistent with applicable laws.

1. I certify that I have read and understand the Policy and Procedures (the "Policy"), and agree to abide by the Policy's terms.

2. I agree to access, use or disclose protected health information only as needed to perform my job, and I will not use or disclose such information to persons or organizations who are unauthorized to have such information.

3. I agree that I will use due care in verifying the identity of anyone claiming to have authorization to obtain confidential patient information, whether or not such persons are employees of TWCCH.

4. I understand that patient information belongs to the patient and that I am only the caretaker and must guard the information appropriately. This includes, but is not limited to, keeping patient information secure, private, and out of public viewing, protecting computerized data by logging off when leaving a work station, and keeping information secure by not discussing patient specific issues in public areas such as elevators and lobbies.

5. When using patient information for authorized purposes, or when disclosing such information to authorized individuals, I agree to use or disclose only the minimum necessary amount of patient information required to carry out the task for which the information is being implemented.

6. I agree to seek permission of the HIPAA Compliance Officer to copy documents containing confidential patient information for any purpose. I agree not to access, copy or download confidential patient information for any purpose other than that of performing my job.

7. I understand that there can be serious legal consequences if I do not keep patient information confidential, or if I allow or participate in the inappropriate dissemination of or access to patient care information.

8. I understand that if I fail to comply with the terms of this Statement and the terms of the Policy, I will be subject to disciplinary action, including possible termination of my employment.

9. Any questions concerning this statement or this Policy can be directed to TWCCH's HIPAA Compliance Officer.

10. I certify that I have received training regarding TWCCH's policies and procedures for handling patient information.

I acknowledge that I have received and read this Employee Confidentiality Statement and that I understand my obligations to maintain the confidentiality of patient information. I hereby agree to comply with the guidelines set forth in this Statement and in the Policy.

_____	_____	_____
Employee	Signature	Date

Eff. 11/2018

Appendix A

Compliance Officer Contact Information:

- Name: David Beecham
- Direct Office Phone Number: (570) 343-2383 x 1032
- Email: hipaa@thewrightcenter.org
- Fax: (570) 963-6133
- Office Location: Administration Building
  501 South Washington Avenue, Suite 1000, Scranton, PA
  18505

Appendix B

Disaster Recovery Planning - Standard

This Standard supports and supplements *Primary – IT Security and Assurance Policy*. The Standard is mandatory and enforced in the same manner as the Policy. It will be periodically reviewed and updated as necessary to meet emerging threats, changes in legal and regulatory requirements, and technological advances.

I. Overview

In order to facilitate the backup, recovery, and restoration of the Wright Centers IT infrastructure that support critical business functions and access to data in a timely manner, the IT Department shall engage in disaster recovery planning efforts and ensure that there are adequate data backups based upon data classifications.

IT disaster recovery planning is the ongoing process of planning, developing, implementing, and testing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

Engaging in IT disaster recovery planning ensures that system dependencies and risks have been identified and accounted for when developing the order of recovery, establishing recovery time and recovery point objectives and documenting the roles of required personnel.

Also, to protect against the loss of data in the event of a physical disaster, database corruption, hardware or software failure, or other incident which may lead to the loss of data, the Wright Center requires all organizational data to be backed up in accordance with this standard as an integral component of its disaster recovery plan. These backup requirements will allow business processes, research, and clinical operations to be resumed in a reasonable amount of time with minimal loss of data.

II. Scope

This Standard is applicable to all individuals and departments of the Wright Center. Specifically, the scope of this policy includes:

- Critical IT infrastructure and other services which facilitate the transport, authentication and security of systems and data (e.g. network, firewall, DNS, Active Directory, EMR, File Shares, Print Services, etc.).
- Information technology systems that process or store mission critical data managed by, or on behalf of, the Wright Center, as determined by the unit that maintains the system.
- The processes, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.

Anyone who is responsible for a mission critical system or service must have an IT disaster recovery (DR) plan that documents the critical recovery functions and tasks that can be executed to enable mission critical system recovery following a significant event or disaster.

III. Roles and Responsibilities

Disaster Recovery Leads: VP of IT, Sr. Network Administrator, and Sr. Systems Administrator

- Coordinates organization IT network/systems disaster recovery program.
- Leads to jointly coordinate cohesive Business Continuity and Disaster Recovery plans across the organization;

- Maintains TWC IT disaster recovery planning templates and processes.
- Provides unit-level consulting and support.
- Identify mission critical systems;
- Maintain adequate data backup and restoration processes for mission critical data and the IT systems assigned to them;
- Develop, implement, maintain, and test disaster recovery plans; and
- Update the status of their DR planning annually.
- Work to review DR plans at least annually or whenever significant system architecture or personnel changes occur.
- Brief leadership on status of DR efforts and resources needs.

IV. Definitions:

Mission Critical: Mission critical IT systems provide essential IT functions and access to data that will have an immediate detrimental effect on the Wright Center if the system fails or is interrupted, including, but not limited to, one or more of the following:

1. Risk to human life or safety
2. Significant impact on the TWC's research, learning, clinical, and administrative operations.
3. Significant legal, regulatory or financial costs.
4. Serious impediment to a location or department from carrying out its critical business functions within the first 24 hours following an event (24 hour Recovery Time Objective – RTO).
5. Loss of access to data with defined availability requirements.

Critical Business Functions: Critical operational and/or business support functions that cannot be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing TWC operations.

Recovery Time Objective (RTO): The duration of time within which a business process must be restored and a stated service level achieved following a disruption in order to avoid unacceptable consequences associated with a break in service.

Recovery Point Objective (RPO): The maximum tolerable period in which data might be lost from an IT system or service due to a major incident.

IT Disaster Recovery Planning: The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.

Business Continuity Planning: Business Continuity Planning, as opposed to disaster recovery planning, is the process of developing prior arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption.

V. Standard

- *Critical Systems*: All units that maintain critical information technology systems will develop, implement, and test (exercise) disaster recovery plans for those systems;
- *Disaster Recovery Plan Template*: Disaster recovery plans should follow the general content and guidelines identified in the Disaster Recovery Plan Template.
- *Disaster Recovery Review/Plan Testing*: Disaster recovery plans must be reviewed and tested on an annual basis or whenever a significant change to system architecture, system dependencies or recovery personnel occurs;

- *New System Evaluation*: New applications or systems will be evaluated; for systems determined to be critical, a disaster recovery plan must be documented and tested prior to go live;
- *Risk Assessment:* Disaster recovery plans need to incorporate a risk assessment that identifies potential negative impacts to the mission critical system. In addition, environments designated as mission critical must have a risk assessment (see Risk Management Standard) performed at least every four years or in accordance with the regulatory requirements of the system.
- *Plan Availability*: Plans must be accessible and available, independent of availability of IT systems.

The following table should be used to determine IT disaster recovery requirements for systems or machines based on:

1. Level of criticality as defined above.
2. Classification levels of information Restricted, High, Moderate, Low.

Table 1: Disaster Recovery Requirement Table by RTO and Sensitive Data Classifications

RTO Information Classification	**RTO**	**RPO**	**Response Time Objective**	**DR Plan Requirements**
Platinum (critical) Mission Critical	1 hour	No data loss except data in transit	Best possible performance, required, robust real-time transaction speed monitoring	Required
Gold (critical) High / Restricted	4 hours	24 hours	Better performance, some transaction monitoring	Required
Silver Moderate	1-30 days	1-7 days	No performance targets, Not monitored	Recommended
Bronze Low	> 1 months or no recoverable	1 month or risk of entire loss	Economy performance, not monitored	Recommended

Data Backup Requirements

Backups are:

- Required for all mission critical systems and for any system or machine that processes, maintains, or stores high or restricted data.
- Required for individual staff, particularly if the data has value as intellectual property and cannot be recreated in a timeframe satisfactory to the owner.
- Recommended for any system or machine that processes, maintains, or stores moderate data.
- Optional for all other systems or data.

It is the responsibility of TWC IT Department to:

- Identify primary responsibility within the unit for data backup; Appropriate roles and responsibilities must be defined for data backup and restoration to ensure timeliness and accountability.

- Classify organizational data based on TWC's information classifications and determine the backup method best suited to their classification level (see Table 2 below).
- Ensure that backups containing information classified as high and restricted are encrypted both in transit and at rest; It is recommended that information classified as moderate are also encrypted.
- Ensure that backups are secure, regularly validated and accessible, and created using a methodology and frequency that meets the desired Recovery Time/Recovery Point Objectives (RTO/RPO), as defined in this Standard.

Table 2: Information Backup Requirement Based on Information Classification Level and RTO
The following table should be used to determine backup requirements for systems or machines that process, maintain, or store moderate, high, or restricted information and for mission critical systems, regardless of the information classification. Where information can be classified into more than one of the categories listed below, the classification with the most stringent information backup requirements must be met.

Information Classification	**Information Backup Requirements**	**Recovery Point Objective (RPO)**	**Recovery Time Objective (RTO)**	**Information Backup Encryption**
Restricted	Required	0 - 24 hours	24 - 48 Hours	Required - At rest / in transit
High	Required	0 - 24 hours	24 - 48 Hours	Required - At rest / in transit
Moderate	Recommended	0 - 24 hours	7 - 30 days	Recommended
Low	Recommended	0 - 24 hours	> 1 month or non-recoverable	Optional
Recovery Time Objective Classification				
Platinum	Required	No data loss except data in transit	4 hours	Recommended
Gold	Required	0 - 24 hours	24 - 48 Hours	Optional
Silver	Recommended	1 - 7 days	7 - 30 days	Optional
Bronze	Recommended	1 month or risk of entire loss	> 1 month or non-recoverable	Optional

VI. Third Party Vendors

It is the responsibility of the IT Department to ensure that contracts with TWC vendors that maintain, protect or provide access to TWC mission critical or moderate, high, or restricted data include disaster recovery and data backup, and Service Level Agreements.

VII. Violations and Sanctions

Any department or individual found to operate in violation of this Standard may be held accountable for remediation costs associated with a resulting information security incident or other regulatory non-compliance penalties, including, but not limited to, financial penalties, legal fees, and other costs.

Violations of this Policy and supplemental documentation and standards may be subject to disciplinary action.

VIII. Implementation

The IT Department is responsible for the interpretation of this Standard.

Appendix C

Security Log Collection, Analysis, and Retention - Standard

This Standard supports and supplements *Primary – IT Security and Assurance Policy*. The Standard is mandatory and enforced in the same manner as the Policy. It will be periodically reviewed and updated as necessary to meet emerging threats, changes in legal and regulatory requirements, and technological advances.

I. Overview

In order to fulfill the Wright Center's obligation to ensure the security and privacy of its information and protection of its systems it is necessary to appropriately generate, store, and analyze network, system, and application log data. System and application log data are a critical component in detecting, analyzing, preventing, and responding to potential information security incidents including unauthorized data disclosures and activities on TWC systems.

The key objectives of this Standard are to:

- Ensure that an appropriate log collection and analysis infrastructure is in place so that information security incidents can be detected and responded to in a timely manner; and
- Ensure that appropriate log collection, analysis, and retention are in place to satisfy ethical, policy, contractual, and legislative requirements, specifically the federal regulatory requirements of HITECH, HIPAA, and PCI.

II. Scope

This standard is applicable to all departments, individuals, locations, and operations of the Wright Center. Specifically, the scope of this policy includes, but may not be limited to:

- All organizational data, including but not limited to, administrative, educational, clinical, research, or any other data related to the Wright Center.
- Third-party vendors who collect, process, share, transmit or maintain data, whether managed or hosted internally or externally.
- All devices that access or maintain sensitive data.

III. Roles and Responsibilities

IT Department

- Collaborates and coordinates to develop and implement security log procedures.
- Coordinates in the event that there is a need to examine or collect log data from a specific device or system.
- Coordinates review and release of security log data across the Wright Center and to law enforcement agencies. Helps law enforcement interpret the data.
- Assists and advises in responding to internal or external requests to access security logs to ensure that the most accurate and relevant log data is released.
- Provides detailed technical and procedural guidance for implementation of this Standard.

Departments:

- Adhere to the requirements of this Standard in all instances where logging of systems or applications include moderate, high or restricted data.
- Protect the confidentiality, integrity, and availability of security logs within their control.
- Maintain awareness of and compliance with regulatory log collection and analysis requirements that apply to the types of data within the department, e.g., HIPAA, PCI, etc.
- Provide log data to the IT Department upon request for incident detection, incident response, and to satisfy policy and regulatory requirements.

IV. Standard

Security Logs are records of events occurring within the Wright Center's computer information systems and networks. A security log captures information associated with information security related events, and can identify anomalies for further analysis and potential remediation.

Security logs are a type of IT security information and are classified as High (Level 3) information. Systems that aggregate and process security logs must be protected in a manner consistent with this data classification.

Logging must be enabled at the operating system, application and database, and system levels when moderate, high or restricted data are processed, maintained, transmitted, or stored. It is recommended that logging is enabled for systems, applications, and databases that maintain low data.

All log data for systems, devices, and applications must be collected and stored as outlined below when technically feasible:

Log Configuration and Management:

- **Activities to be Logged:** Logs must include at least these auditable events:
  - Successful and unsuccessful logins and authentication
  - Authorization failures
  - Password changes
  - Modification of security settings
  - Group membership changes
  - System or network configuration changes
  - Access control changes
  - User access to high or restricted data
  - User modification of high and restricted data (e.g., configuration of sensitive or critical systems, financial transactions)
  - Privileged actions, such as those actions requiring administrator, sudo, or root access.
  - Detection of suspicious or malicious activity from IT security systems, such as from an intrusion detection system or antivirus system.

- **Log Elements:** All relevant log events must contain the following:
  - True source and/or destination IP address regardless of network address translation
  - User identification: Username for authenticated user that is responsible for the action being logged (when logging user activity)
  - Accurate timestamp for the event
  - Type of event
  - Description of attempted or completed activity

- Precise identification of resource being acted on (e.g., filename with full path, hostname of device, etc.)

- **Centralized Log Collection and Review:**
  - Log data from departments and individuals encompassing high or restricted data must be forwarded to a centralized syslog or event monitoring server when technically feasible.
  - Forwarding of data should be in real time
  - Logs should be saved to a secure server or an off-site location
  - Monitoring and real-time alerting should be implemented to detect conditions that may negatively impact the integrity or availability of log data.

- **Log Data Integrity:**
  - Log information must be protected from unauthorized changes and operational problems. Rights to insert, modify, and delete user identifiable audit log records must be strictly controlled.
  - Audit log records should contain the identity of the source of an insert, modification or deletion of a user identifiable audit log record.
  - Individuals must not be assigned to be the sole reviewers of their own activity, and should not have permission to erase, deactivate, or modify logs of their own activities.

- **Log Data Access Control and Confidentiality:**
  - Appropriate access controls must be implemented to ensure that only authorized individuals have access to sensitive log data. Individuals must be granted access to security logs on a least privilege basis, and only to staff members with a job-related need for such access.
  - User access to sensitive log data should be reviewed and audited on an annual basis.
  - Rights to view or run reports from user identifiable audit log data must be strictly controlled.
  - The identity of the user accessing, viewing and running reports from user identifiable audit log data should be logged.

- **Log Data and Forensic Investigations:**
  - The information captured by logs can be used to support incident response and as part of a forensic investigation in the event of a suspected data breach or other forms of electronic crime.

Privacy and Security Logs

Security logs will generally be used for their intended purpose as they are described throughout this document. However, in the event of a declared health or safety emergency, the IT Department or a delegated authority may authorize accessing information contained in security logs.

In some cases, the Wright Center may be compelled by law, such as a court order, subpoena, or other legal reasons to retain or release information contained in security logs. All such releases are coordinated by IT Department.

Security Log Retention

Security logs of systems, networks, and applications that process, maintain, transmit, or store TWC information with a moderate to restricted classification must be retained for 1 year unless longer retention times are required by law or contractual obligation or unless exception is provided.

Security logs that no longer need to be retained should be disposed of by following the procedures detailed *Supplemental – Electronic Data Disposal and Media Sanitization.*

IV. Exceptions

Exceptions to the required minimum standards for handling security logs, with or without personally identifiable information, are expected to be generally in line with the provisions of *Supplemental – Request for Exceptions.*

V. Violations and Sanctions

Any department or individual found to operate in violation of this Standard may be held accountable for remediation costs associated with a resulting information security incident or other regulatory non-compliance penalties, including, but not limited to, financial penalties, legal fees, and other costs. This also applies to violations of personally owned devices where the device owner may be held accountable in the same manner as above.

Anyone who violates these standards or supplemental documentation may be subject to appropriate disciplinary action.

VI. Implementation

IT Department is responsible for the interpretation and maintenance of this standard.