

Resolution

Number 25-0235

Adopted Date February 25, 2025

HIRING MELODY ROTH AS ELIGIBILITY REFERRAL SPECIALIST II, WITHIN THE WARREN COUNTY DEPARTMENT OF JOB AND FAMILY SERVICES, HUMAN SERVICES DIVISION


BE IT RESOLVED, to hire Melody Roth, as Eligibility Referral Specialist II, within the Warren County Department of Job and Family Services, Human Services Division, classified, full-time permanent, non-exempt status (40 hours per week), Pay Grade #12, \$20.03 per hour, under the Warren County Job and Family Services compensation plan, effective March 3, 2025, subject a negative background check, drug screen and a 365-day probationary period.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

H/R

cc: Human Services (file)
M. Roth's Personnel file
OMB – Sue Spencer

Resolution

Number 25-0236

Adopted Date February 25, 2025

APPROVING THE END OF A 365-DAY PROBATIONARY PERIOD AND A PAY INCREASE FOR SHYANNE MCELLEY WITHIN THE DEPARTMENT OF JOB AND FAMILY SERVICES, CHILDREN SERVICES DIVISION

WHEREAS, Shyanne McElley, Investigative Caseworker II, within the Department of Job and Family Services, Children Services Division, has successfully completed a 365-day probationary period.

NOW THEREFORE BE IT RESOLVED, to approve Shyanne McElley's completion of 365-day probationary period and a pay increase to rate of \$25.62 hourly, effective pay period beginning March 8, 2025.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Children Services (file)
S. McElley's Personnel File
OMB – Sue Spencer

Resolution

Number 25-0237

Adopted Date February 25, 2025

APPROVING THE END OF A 365-DAY PROBATIONARY PERIOD AND A PAY INCREASE FOR MINDY ADAMS WITHIN THE DEPARTMENT OF JOB AND FAMILY SERVICES, HUMAN SERVICES DIVISION

WHEREAS, Mindy Adams, Administrative Support, within the Department of Job and Family Services, Human Services Division, has successfully completed a 365-day probationary period.

NOW THEREFORE BE IT RESOLVED, to approve Mindy Adams' completion of 365-day probationary period and a pay increase to rate of \$19.23 hourly, effective pay period beginning March 8, 2025.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Human Services (file)
M. Adams' Personnel File
OMB – Sue Spencer

Resolution

Number 25-0238

Adopted Date February 25, 2025

ADMINISTERING DISCIPLINARY ACTION AGAINST JEREMY TURNMIRE WITHIN THE WARREN COUNTY WATER AND SEWER DEPARTMENT

WHEREAS, Mr. Turnmire, was charged with his third Group I Offense #15, Failure to observe departmental rules, procedures, and/or practices, and Group I Offense #20, Unsatisfactory work or failure to maintain required standards of performance, in accordance with the Warren County Personnel Policy Manual; and

WHEREAS the Sanitary Engineer requested a pre-disciplinary conference for the above violations; and

WHEREAS, Mr. Turnmire was given notice of a pre-disciplinary conference on February 13, 2025; and

WHEREAS, Mr. Turnmire waived his right to a pre-disciplinary conference on February 13, 2025; and

WHEREAS, it is the recommendation of the Sanitary Engineer that Mr. Turnmire serve a one (1) day suspension without pay.

NOW THEREFORE BE IT RESOLVED, that Jeremy Turnmire, Water Treatment Plant Operator I, within the Warren County Water and Sewer Department, be disciplined for violating the Warren County Personnel Policy Manual as herein before discussed, the penalty for which shall consist of a one (1) day suspension to be served February 26, 2025; and

BE IT FURTHER RESOLVED, this action shall become a part of Mr. Turnmire's personnel file.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS


Ashley Watts, Deputy Clerk

cc: Water and Sewer (file)
J. Turnmire's Personnel File
OMB (Sue Spencer)

Resolution

Number 25-0239

Adopted Date February 25, 2025

AUTHORIZING SECTION 111 MANDATORY REPORTING PROFILE REPORT RELATIVE TO WORKERS COMPENSATION

WHEREAS, authorization is needed on the Section 111 Mandatory Reporting Profile relative to the workers' compensation program and transmission and safeguards of claim data exchange for the purpose of complying with the Medicare Secondary Payor Mandatory Reporting provisions.

NOW THEREFORE BE IT RESOLVED, to authorize Section 111 Mandatory Reporting Profile Report attached hereto and made a part hereof.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

HR/

cc: Sedgwick CMS
Anthony Henry, EDI Representative
Tammy Whitaker, OMB
Workers' Compensation File

Resolution

Number 25-0240

Adopted Date February 25, 2025

**ACKNOWLEDGING UPDATE TO THE HIPAA POLICY AND ATTESTATION RELATIVE
TO REPRODUCTIVE HEALTH CARE AND SUBSTANCE USE DISORDER PATIENT
RECORD REGULATIONS**

WHEREAS, an update is needed to the HIPAA Policy due to changes in the HIPAA Privacy Rule that includes PHI protections related to reproductive health care, as well as modification of the Confidentiality of Substance Use Disorder Patient Record Regulation; and

WHEREAS, these changes include an accompanying Attestation regarding requested use or disclosure of protected health information relative to reproductive health care and substance use.

NOW THEREFORE BE IT RESOLVED, to acknowledge updates needed to the HIPAA Policy and associated Attestation relative to reproductive health care and substance and use disorder regulations, as attached hereto and made a part hereof.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS


Ashley Watts, Deputy Clerk

HR/

cc: HUB Heartland
Tammy Whitaker, OMB
Benefits File
Policy file

Warren County

Attestation Regarding a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care

Instructions:

Covered entities and their business associates may not use or disclose PHI for the following purposes:

- (1) To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- (2) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- (3) To identify any person for any purpose described in (1) or (2).

The prohibition applies when the reproductive health care at issue (1) is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided, (2) is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided, or (3) is provided by another person and presumed lawful.

The Privacy Rule requires Warren County as a Plan Sponsor of a covered health plan to obtain a written attestation where a request is made under the Privacy Rule permissions at 45 CFR 164.512(d) (disclosures for health oversight activities, disclosures for judicial and administrative proceedings, disclosures for law enforcement purposes, or disclosures about decedents to coroners and medical examiners).

- By signing this attestation, you are verifying that you are not requesting PHI for a prohibited purpose and acknowledging that criminal penalties may apply if untrue.
- You may not add content to the attestation that is not required or combine this form with another document except where another document is needed to support your statement that the requested disclosure is not for a prohibited purpose.
 - For example, if the requested PHI is potentially related to reproductive health care that was provided by someone other than the covered entity or business associate from whom you are requesting the PHI, you may submit a document that supplies information that demonstrates a substantial factual basis that the reproductive health care in question was not lawful under the specific circumstances in which it was provided.
- Any documentation that may be added to support the statements given as part of the attestation or to overcome the presumption of lawfulness as explained above must be separately appended to the attestation.

**Attestation Regarding a Requested Use or Disclosure of Protected Health Information
Potentially Related to Reproductive Health Care**

Name of person(s) or specific identification of the class of persons to receive the requested PHI.
Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure.
Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals whose protected health information you are requesting.

I attest that the use or disclosure of PHI that I am requesting is not for a purpose prohibited by the HIPAA Privacy Rule at 45 CFR 164.502(a)(5)(iii) because of one of the following (check one box):

- The purpose of the use or disclosure of protected health information is **not** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes.
- The purpose of the use or disclosure of protected health information **is** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was **not lawful** under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person.

Signature of the person requesting the PHI

Name: _____ Date: _____

If you have signed as a representative of the person requesting PHI, provide a description of your authority to act for that person.

HIPAA

(Health Insurance Portability and Accountability Act of 1996)

**Privacy & Security Policies and Procedures
for
Warren County, Ohio
Organized Health Care Arrangements**

Table of Contents

Introduction -4-

PART I. Definitions & General Policies - 5 -

A. Definitions.....- 6 -

B. Compliance with HIPAA Rules- 9 -

C. Privacy Officer- 10 -

D. Security Officer.....- 12 -

E. Training.....- 15 -

F. Plan Documents.....- 17 -

G. Business Associates- 19 -

H. Breach Notifications- 21 -

PART II. Privacy Policies.....- 24 -

A. Permitted Uses and Disclosures of PHI.....- 25 -

B. Disclosures to Plan Sponsor.....- 34 -

C. Minimum Necessary Standard- 35 -

D. Written Authorizations.....- 37 -

E. Oral or Implicit Permission to Disclose PHI- 39 -

F. Disclosures Requiring Attestation- 41 -

G. De-Identified Information.....- 44 -

H. Requests for Restrictions on Use or Disclosure of PHI.....- 45 -

I. Requests for Confidential Communications.....- 47 -

J. Right of Access to PHI- 49 -

K. Right to Request Amendment of PHI- 51 -

L. Right to Request an Accounting of Disclosures- 54 -

M. Sanctions for Violating the Privacy Rule- 57 -

N. Privacy Complaints- 58 -

O. Mitigation of Harm Due to Improper Uses or Disclosures.....- 60 -

P. No Retaliation or Intimidation.....- 61 -

Q. No Waiver of Rights- 62 -

R. Notice of Privacy Practices- 63 -

PART III. Security Policies- 64 -

A. Risk Analysis- 65 -

B. Risk Management- 66 -

C. Sanctions for Violating the Security Rule- 67 -

D. User Access Management.....- 69 -

E. Authentication & Password Management.....- 72 -

F. Log-In Monitoring- 73 -

G. Facility Access Controls.....- 74 -

H. Workstation Use & Security- 75 -

I. Device & Media Controls- 76 -

J. Transmission Security- 77 -

K. Protection From Malicious Software- 78 -
L. System Audits, Audit Controls & Activity Review.....- 79 -
M. Response and Reporting.....- 80 -
N. Contingency Plan.....- 82 -
O. Disposal of ePHI.....- 84 -

Introduction

Warren County, Ohio (the "Plan Sponsor") provides various group health benefits to eligible employees and their eligible dependents. These benefits are provided under a group health plan or plans as identified from time to time by the Plan Sponsor that are "Covered Entities" as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Office of the Secretary of the Department of Health and Human Services (the "Secretary") has issued: (1) regulations providing Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Subparts A and E of Part 164 (the "Privacy Rule"); (2) regulations providing Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Subpart C of Part 164 (the "Security Rule"); and (3) regulations modifying the Privacy Rule, Security Rule, Enforcement and Breach Notification Rules (collectively the "HIPAA Rules").

The privacy and security provisions of HIPAA have been amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009, and any and all references herein to the "HIPAA Rules" shall be deemed to include the Privacy Rule, the Security Rule, HITECH, the Enforcement and Breach Notification Rules, and all existing and future implementing regulations, as they become effective.

These policies and procedures (the "Policies") apply to each self-funded group health benefit and to each fully-insured group health benefit, to the extent the Plan Sponsor receives Protected Health Information ("PHI") for administration of such benefit and is required to maintain policies and procedures under the HIPAA Rules.

These Policies outline the obligations of the Plan and the Plan Sponsor as well as the rights of appointing authorities, employees, and dependents participating in the Plan under the HIPAA Rules. The Plan and the Plan Sponsor intend to comply fully with the requirements under the HIPAA Rules with respect PHI Used or Disclosed by the Plan. These Policies have been adopted by the Plan Sponsor for purposes of complying with the HIPAA Rules with respect to the Plan, but these Policies do not create third party rights for or with respect to Participants, business associates or otherwise.

The Plan Sponsor reserves the right to amend these Policies at any time. These Policies should be interpreted in a manner consistent with the HIPAA Rules. To the extent the Policies contain requirements or duties that are not required under the HIPAA Rules, such requirements or duties are not binding and are to be interpreted solely as goals. The Plan Sponsor does not intend for the Policies to create additional requirements or obligations on the Plan Sponsor, the Plan or any employees that are not imposed by the HIPAA Rules.

PART I

DEFINITIONS & GENERAL POLICIES

A. Definitions

In applying the policies and procedures (including Parts I through III), the following definitions shall apply. Any capitalized term not defined below shall have the meaning set forth in the HIPAA Rules.

1. "Breach" means an unauthorized acquisition, access, or use or disclosure of unsecured PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of such information. A Breach excludes the following:
 - a. any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Plan or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Rules;
 - b. any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Rules; or
 - c. a disclosure of PHI where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
2. "Designated Record Set" means a group of records maintained by or for the Plan that include:
 - a. medical and billing records about Participants maintained by or for a covered health care provider;
 - b. the enrollment, payment, claims adjudication and care or medical management records systems maintained by or for the Plan; and
 - c. that are used in part or in whole by or for the Plan to make decisions about Participants.
3. "Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
4. "Electronic Media" means:
 - a. Electronic storage material on which data is or may be recorded electronically, including, for example, 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
 - b. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet

or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, if the information being exchanged did not exist in electronic form immediately before the transmission.

5. "Electronic Protected Health Information" or "Electronic PHI" means PHI that is transmitted by or maintained in Electronic Media.
6. "Employee Benefits Representative" means all County Employee Benefits Department personnel and certain Human Resources personnel whose responsibilities include day-to-day healthcare benefit administration.
7. "Individually Identifiable Health Information" means health information that: (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and (3) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
8. "Plan" means the health care plan components of the Warren County Employee Health Care Plan.
9. "Plan Sponsor" means Warren County, Ohio.
10. "Privacy Officer" means the Benefits Coordinator in the County Office of Management and Budget.
11. "Protected Health Information" or "PHI" means Individually Identifiable Health Information, but excludes employment records held in the role of an employer and information regarding a person who has been deceased for more than 50 years. Accordingly, PHI includes Individually Identifiable Health Information that is received or maintained by the Plan Sponsor in the performance of plan administration functions for the Plan, but PHI does not include information that is received or maintained by the Plan Sponsor in its capacity as the employer of a participant or beneficiary. PHI also includes genetic information.
12. "Reproductive Health Care" means health care that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes which includes but is not limited to contraception, including emergency contraception; preconception screening and counseling; management of pregnancy and pregnancy-related conditions, including pregnancy screening, prenatal care, miscarriage management, treatment for preeclampsia, hypertension during pregnancy, gestational diabetes, molar or ectopic pregnancy, and pregnancy termination; fertility and infertility diagnosis and treatment, including assisted reproductive technology and its components (e.g., in vitro fertilization (IVF)); diagnosis and treatment of conditions that affect the reproductive system (e.g., perimenopause, menopause, endometriosis, adenomyosis); and other types of

care, services, and supplies used for the diagnosis and treatment of conditions related to the reproductive system (e.g., mammography, pregnancy-related nutrition services, postpartum care products).

13. "Security Officer" means the Warren County Automatic Data Processing Board as defined in Ohio Revised Code 307.847.
14. "Summary Health Information" means information that may be Individually Identifiable Health Information and that summarizes the claims history, claims expenses, or types of claims experience by participants in the Plan, provided that the 18 specific identifiers in 45 CFR § 164.514(b)(2)(i) are removed, except that geographic information need only be aggregated to the level of a five digit zip code.
15. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS.

B. Compliance with HIPAA Rules

POLICY:

The Plan will comply fully with the requirements of the HIPAA Rules. No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by these policies and procedures. The Plan reserves the right to amend or change any of the policies or procedures at any time (and even retroactively) without notice. To the extent that these policies and procedures establish requirements and obligations above and beyond those required by HIPAA, the policies and procedures shall be aspirational and shall not be binding upon the Plan. These policies and procedures do not address requirements under state law or federal laws other than HIPAA.

PROCEDURES:

1. The Plan's privacy and security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the privacy and security of PHI, and any changes to policies or procedures will be documented promptly.
2. Except to the extent that they are carried out by the Plan Sponsor or business associates, the Plan shall document certain actions, activities, and assessments with respect to PHI required by HIPAA to be documented (including amendment of the Plan document in accordance with this policy, for example).
3. Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.
4. The Plan will make its policies, procedures, and other documentation available to the Privacy Officer, Security Officer, Plan Sponsor, third-party administrators and other business associates or other persons responsible for implementing the procedures to which the documentation pertains.

C. Privacy Officer

POLICY:

The Plan's Privacy Officer is responsible for the development and implementation of the Plan's policies and procedures relating to privacy, as well as the Plan's maintenance of and adherence to those policies and procedures.

PROCEDURES:

The Privacy Officer's responsibilities are as follows:

1. Take the lead role and assist in the formation, implementation, and maintenance of these privacy policies and procedures.
2. Maintain and ensure proper distribution of the privacy notice.
3. Perform periodic reviews of the uses and disclosures of the Plan's PHI.
4. Perform or supervise the delivery of privacy training to the Plan's workforce members.
5. Take a lead role and assist in drafting appropriate business associate agreement provisions, assist in identifying business associate service providers, and develop appropriate monitoring under the Privacy Rule of business associate agreements.
6. Implement and oversee the administration of participant and beneficiary rights under the Privacy Rule, including the right to access, right to request amendment, right to an accounting, and the right to request privacy protections.
7. Implement a process for tracking all disclosures of PHI that must be tracked and accounted for (upon participant or beneficiary request) under the Privacy Rule.
8. Establish and administer a system for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Plan's privacy policies and procedures or compliance with the Privacy Rule.
9. Monitor legal changes and advancements in technology to ensure continued compliance.
10. Maintain (or supervise the maintenance of) all documentation required by the Privacy Rule.
11. Establish sanctions for failure to comply with the group health plan's privacy policies and procedures.
12. Cooperate with the U.S. Department of Health and Human Services, Office of Civil Rights, and other legal entities in any compliance reviews or investigations.
13. Be the official contact and information source for all issues or questions relating to the Plan's privacy treatment of participant and beneficiary PHI.

14. Work with the Security Officer for the Plan to ensure appropriate coordination between the health privacy and security programs, including compliance with the requirements of the HITECH Act to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of the business associates discover a Breach.
15. In cooperation with the Security Officer, develop and oversee the training of appropriate members of the Plan Sponsor's workforce regarding the Privacy Rule, as well as privacy policies and procedures for the Plan.
16. Work with the Security Officer to investigate and resolve security Breaches involving Electronic PHI of the Plan, including Breaches reported by business associates.
17. Undertake any other activities relating to PHI that are necessary or desirable to comply with the HIPAA Rules.

D. Security Officer

POLICY:

The Plan's Security Officer is responsible for the development and implementation of the Plan's policies and procedures relating to the Security Rule, as well as the Plan's maintenance of and adherence to those policies and procedures.

PROCEDURES:

The Security Officer's responsibilities are as follows:

1. Perform initial and periodic written risk assessments related to security of Electronic PHI for the Plan.
2. Implement, oversee, and monitor risk management measures to address security risks and vulnerabilities identified by risk assessments performed for the Plan, including the development and updating of a comprehensive written risk management program for the Plan.
3. Apply standard corporate security policy and procedures providing the framework and the measures to protect against reasonably anticipated threats or hazards to security or integrity of Electronic PHI of the Plan.
4. Apply standard corporate security policy and procedures providing the framework and the measures to protect against reasonably anticipated unauthorized uses or disclosures of Electronic PHI of the Plan.
5. Facilitate the Plan Sponsor's and Plans' compliance with:
 - a. the Security Rule; and
 - b. all Plan HIPAA security policies and procedures.
6. Oversee the development, implementation, and maintenance of appropriate security policies and procedures for the Plan.
7. Oversee the development, implementation, and maintenance of appropriate documents and forms, including:
 - a. security policies;
 - b. business associate contracts; and
 - c. other policies, forms, and documentation required by HIPAA.

8. Apply standard corporate policies and procedures to regularly review records of computer or information system activity relating to the Plan, such as audit logs, access reports and security incident tracking reports.
9. Review and maintain standard corporate security policies to ensure that they address the security of Electronic PHI of the Plan, including:
 - a. systems/processes to monitor, track and index Electronic PHI;
 - b. information system access and activity (e.g. audit logs, access reports);
 - c. appropriate administrative, technical, and physical security measures;
 - d. compliance with the Security Rule; and
 - e. the retention of all required documentation for at least six years.
10. Apply standard corporate security policy and procedures for the authorization of Plan Sponsor's workforce members who have access to Electronic PHI and develop and implement PHI, procedures to terminate access when the Plan Sponsor's workforce members are terminated or transferred to other positions at the Plan Sponsor in which their access to Electronic PHI would be inappropriate.
11. Apply standard corporate security policy and procedures for granting access authorization to areas where Electronic PHI of the Plan is stored or used and for computers on which such Electronic PHI is stored or used, including password management and similar issues.
12. Apply standard corporate security policy and procedures in cooperation with other Plan Sponsor employees, for data backup procedures, disaster recovery plans, and emergency mode plans for the Plan.
13. Apply standard corporate security policies and procedures for physical and technical safeguards.
14. Work with business associates of the Plan on HIPAA security issues and concerns.
15. Conduct periodic review of security policies and procedures for the Plan and update as needed in response to environmental or operational changes.
16. Work with legal counsel to ensure that policies, procedures, forms, and other documents of the Plan comply with the Security Rule and that the appropriate amendments have been made to these documents.
17. Coordinate work of other Plan Sponsor departments on security issues relating to the Plan, such as IT and security departments.
18. Work with the Privacy Officer for the Plan to ensure appropriate coordination between the health privacy and security programs, including compliance with the requirements of the

HITECH Act to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of the business associates discover a Breach.

19. In cooperation with the Privacy Officer, develop and oversee the training of appropriate members of the Plan Sponsor's workforce regarding the Security Rule, as well as security policies and procedures for the Plan.
20. Provide periodic security updates to remind and update workforce members on the Plan's security policies and procedures.
21. Work with the Privacy Officer to investigate and resolve security Breaches involving Electronic PHI of the Plan, including Breaches reported by business associates.
22. Maintain awareness of changes in security risks, security measures, and computer systems relating to the Plan.
23. Work with senior management to oversee the implementation of a sanction policy and appropriate sanctions for violation of the security policies and practices of the Plan, or for violation of the Security Rule.
24. Cooperate with the Office for Civil Rights (OCR), or other appropriate entity, in any compliance review, audit or investigation of the Plans.
25. Undertake any other activities relating to the Plans that are necessary or desirable to comply with HIPAA Rules.

E. Training

POLICY:

Employees of the Plan Sponsor who are considered part of the Plan's "workforce" will be trained to understand and implement the Plan's privacy policies and procedures and the Privacy Rule.

Employees of the Plan Sponsor who access, receive, transmit or otherwise use Electronic PHI or who set up, manage or maintain systems and workstations that access, receive, transmit, or store Electronic PHI will be trained to understand and implement the Plan's security policies and procedures and the Security Rule.

PROCEDURES:

1. The Privacy Officer and Security Officer have responsibility for implementation of this policy. They are responsible for conducting a training needs assessment and developing and approving a training strategy. They will monitor and periodically evaluate the training plan and modify as necessary.
2. Timing of Training.
 - a. Within a reasonable time after becoming a workforce member.
 - b. Within a reasonable time after material changes to the Plan's privacy policies and procedures.
 - c. Whenever, in the determination of the Privacy Officer or Security Officer, additional training is necessary to ensure compliance with the Plan's privacy and security policies and procedures or the HIPAA Rules.
3. Plan sponsor employees who require privacy training will be trained in the following areas:
 - a. At the determination of the Privacy Officer, on all of the Plan's policies and procedures, or, if appropriate, relevant policies and procedures for any particular employee if his or her job responsibilities do not necessitate training in all of the policies and procedures;
 - b. Permissible uses and disclosures of PHI;
 - c. Relevant provisions of the Privacy Rule; and
 - d. The requirement that all employees report any potential violations of the Plan's policies and procedures or the Privacy Rule, whether caused by a workforce member or a service provider, to the Privacy Officer.
4. Plan sponsor employees who require security training will be trained in the following areas:

- a. At the determination of the Security Officer, on all of the Plan's policies and procedures, or, if appropriate, relevant policies and procedures for any particular employee if his or her job responsibilities do not necessitate training in all of the policies and procedures;
 - b. Confidentiality, integrity and availability;
 - c. Common security threats and vulnerabilities;
 - d. Relevant provisions of the Security Rule; and
 - e. Incident response and reporting procedures.
5. Documentation. The Privacy Officer and Security Officer will maintain records indicating who has been trained, what training occurred, and the date of training, for six years following the date of the training. These documents will be maintained by the Plan.

F. Plan Documents

POLICY:

Before the Plan discloses any PHI to the workforce of the Plan Sponsor for plan administrative functions, the Plan Sponsor shall certify to the Plan that the Plan documents have been amended as required by the HIPAA Rules.

PROCEDURES:

1. For purposes of complying with the Privacy Rule, the certification should represent that the Plan documents require the Plan Sponsor to:
 - a. Not use or further disclose PHI other than as permitted by the Plan or as required by law.
 - b. Ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Company.
 - c. Not use or disclose PHI for employment-related actions.
 - d. Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.
 - e. Make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures.
 - f. Make the Company's internal practices and records relating to the use and disclosure of PHI received from the Plan available to HHS upon request.
 - g. If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
2. For purposes of complying with the Security Rule, the certification should represent that the Plan documents require the Plan Sponsor to:
 - a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Plan.
 - b. Ensure that reasonable and appropriate security measures support the Plan document provisions providing for adequate separation between the Plan and the Plan Sponsor.

- c. Ensure that agents to whom the Plan Sponsor provides Electronic PHI agree to implement reasonable and appropriate security measures to protect the Electronic PHI of the Plan.
- d. Report to Security Officer any security incident of which the Plan Sponsor becomes aware.

G. Business Associates

POLICY:

The Plan Sponsor has many contractual and business relationships. The Plan's relevant service provider contract will incorporate business associate contract language. However, not all contractors or business partners are "Business Associates" as defined by the HIPAA Rules. This policy only applies to contractors or business partners that come within the definition of a "Business Associate."

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this policy. All questions should be addressed, in the first instance, by the Privacy Officer.
2. Business associate contracts.
 - a. All of the Plan's service providers who are business associates under the Privacy Rule must have written contracts.
 - b. The Privacy Officer will ensure that service provider contracts incorporate appropriate business associate language. The Privacy Officer may develop standard business associate contract language but is not required to use such language in all situations.
 - c. The Plan Sponsor will be the signatory on all business associate contracts.
3. The business associate agreements will obtain satisfactory assurances from all business associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA privacy and security regulations and specifically providing:
 - a. The permitted uses and disclosures of PHI by the business associate.
 - b. The prohibition of other uses and disclosures of PHI by the business associate.
 - c. The business associate will make PHI available to satisfy the participant access, amendment and accounting provision standards.
 - d. The business associate will make its records available to HHS for any investigation.
 - e. The business associate will implement appropriate safeguards to prevent unauthorized disclosures of PHI.
 - f. The business associate will implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that the

business associate creates, receives, maintains, or transmits on behalf of the Plan (the Contract Electronic PHI).

- g. The business associate will ensure that any agents or subcontractors to whom the business associate provides PHI agree to the same restrictions and conditions that apply to the business associate and that they implement reasonable and appropriate security measures to protect the Contract Electronic PHI.
 - h. To the extent the business associate is to carry out any of the Plan's obligations under the HIPAA Rules, the business associate will comply with the requirements of the Privacy Rule that apply to the Plan in the performance of such obligation.
 - i. The business associate will report to the Plan any security incident or disclosure of the information other than as provided for by the contract of which the business associate becomes aware.
 - j. The business associate will take required steps with respect to Breach notification requirements.
 - k. The business associate will return or destroy all PHI received from, or created or received by the business associate on behalf of the Plan or, if such return or destruction is infeasible, extend the protections of the contract to the information and limit further uses and disclosures that make the return or destruction infeasible.
 - l. The authorization of the termination of the contract by the Plan if the Plan determines that the business associate has violated a material term of the contract.
4. If the Plan learns of a service provider's potential violation of its business associate contract (either through a participant or beneficiary complaint, during a performance audit, or otherwise), it will take the steps outlined below.
- a. The Privacy Officer will investigate all potential or alleged business associate contract violations and will determine if there is an actual violation.
 - b. Upon determining that there is an actual business associate contract violation, the Privacy Officer will work with the business associate to end the violation or to cure any harm caused. Refer to Plan's Policy and Procedures for Mitigation of Harm.
 - c. If the Privacy Officer determines that the business associate is unwilling to cure or end the violation, then the Privacy Officer will determine if it is feasible to terminate the contract. It is feasible to terminate the contract if there is any other service provider who can supply the same services, even if the cost is higher.

H. Breach Notifications

POLICY:

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a Breach of Unsecured PHI.

PROCEDURES:

1. The Privacy Officer will work with the Security Officer to investigate any impermissible use or disclosure of PHI to determine whether there was a Breach. Acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach, unless the Privacy Officer determines that there is a low probability that the privacy or security of the PHI has been or will be compromised.
2. The Privacy Officer's determination of whether a Breach has occurred must include the following considerations:
 - a. Was PHI involved? If not, there was not a Breach.
 - b. Was Unsecured PHI involved? If not, there was not a Breach.
 - c. Was there unauthorized access, use, acquisition, or disclosure of PHI? If not, then there was not a Breach.
 - d. Is there a low probability that privacy or security was compromised? In order to determine if there is a low probability that the PHI was compromised, the Privacy Officer must perform a risk assessment that considers at least the following factors:
 - i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud; did the disclosure involve information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual or otherwise to further the unauthorized recipient's own interests.
 - ii. The unauthorized person who used the PHI or to whom the disclosure was made. For example, does the unauthorized recipient of the PHI have obligations to protect the privacy and security of the PHI, such as another entity subject to the HIPAA or an entity required to comply with the Privacy Act of 1974 or the Federal Information Security Management Act of 2002, and would those obligations lower the probability that the recipient would use or further disclose the PHI inappropriately? Also, was the PHI

impermissibly used within a covered entity or Business Associate, or was it disclosed outside a covered entity or Business Associate?

- iii. Whether the PHI was actually acquired or viewed. If there was only an opportunity to actually view the information, but the Privacy Officer determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer with was lost or stolen and subsequently recovered, and the Privacy Officer is able to determine (based on a forensic examination of the computer) that none of the information was actually viewed, there may be no probability of compromise.
 - iv. The extent to which the risk to the PHI has been mitigated. For example, if the Plan can obtain satisfactory assurances (e.g., a confidentiality agreement) from the unauthorized recipient of that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.
3. If the Privacy Officer determines that there was not a Breach, the Privacy Officer will document the determination in writing, keep the documentation on file, and is not required to provide notifications, but may notify participants of the violation where appropriate.
 4. If the Privacy Officer determines there was a Breach, the Privacy Officer will provide the required notification to affected individuals.
 - a. The notice will be provided without unreasonable delay and in no event later than 60 days following the discovery of a Breach. A Breach is considered to be discovered on the earlier of (i) the date that a workforce member (other than a workforce member who committed the Breach) knows of the events giving rise to the Breach, or (ii) the date that a workforce member or agent of the Plan would have known of the event giving rise to the Breach by exercising reasonable diligence.
 - b. The notice will be given by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically.
 - c. Notices will be mailed to parents of minor children and to next-of-kin or to a personal representative of a deceased individual.
 - d. Notice will be given by alternative means to individuals whose contact information is out of date. If there are 10 or more individuals with out-of-date contact information, substitute notice will be provided through either a conspicuous posting for a period of 90 days on the homepage of the Plan Sponsor's website or conspicuous notice in major print in the geographic area where the individuals affected by the breach likely reside. If there are fewer than 10 individuals with

out-of-date contact information, substitute notice may be made by telephone, in writing, or by other means.

- e. The notice will contain the following information:
 - i. A description of the Breach, including a brief description of the incident, the types of Unsecured PHI that were involved, the date of the Breach, and the date of the discovery of the Breach;
 - ii. The steps an individual should take to protect themselves from potential harm from the Breach;
 - iii. A description of what the Plan is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and
 - iv. Contact procedures for individuals to ask questions and obtain more information.
- 5. The Security Officer and Privacy Officer will provide the required notification to HHS and will maintain a log of all Breaches.
 - a. If the Breach affects fewer than 500 individuals, notice will be given to HHS no later than 60 days after the end of the calendar year in which the Breach was discovered.
 - b. If the Breach affects 500 or more individuals, notice will be given to HHS without unreasonable delay but in no event later than 60 days following the discovery of a Breach.
- 6. The Security Officer and Privacy Officer will provide notice to the proper media outlets for any Breach that affects 500 or more individuals in a state or jurisdiction. If 500 or more individuals were affected, but not more than 500 residents of any one state or jurisdiction were affected, no notice will be given to the media.
 - a. Notice will be provided in the form of a press release to prominent media outlets in any state or jurisdiction where 500 or more affected individuals reside.
 - b. Notice will be provided without unreasonable delay and in no event later than 60 days following the discovery of a Breach.
 - c. The press release will contain the same information as the information required in the notice to the affected individuals.
- 7. Unless agreed upon otherwise in a Business Associate Agreement, the Security Officer and Privacy Officer will be responsible for following the procedures outlined above if they are notified of a Breach of PHI in the possession of a Business Associate.

PART II

Privacy Policies

A. Permitted Uses and Disclosures of PHI

POLICY:

The uses and disclosures discussed in the procedures below are permitted by the Plan without the participant's or beneficiary's permission or request (written or otherwise), provided the particular requirements of these procedures and the Privacy Rule are met.

PROCEDURES:

1. The following uses and disclosures of the Plan's PHI for "payment" purposes are permitted:
 - . Billing and premium or claims payment
Claims reporting
Claims management and related health care data processing
Utilization review, precertification and preauthorization
Claims inquiries and resolution
Eligibility reporting, enrollment and disenrollment activities
Coverage determination
Determination of cost sharing
Coordination of benefits
Subrogation
Benefit elections
 - a. Additional uses and disclosures may also fall within the Privacy Rule's definition of "payment." The Privacy Officer will determine on a case-by-case basis if a particular use or disclosure not listed above is a payment activity. If that activity is common or recurring, it shall be added to the list above.
 - b. All uses and disclosures of PHI for payment activities will comply with the Plan's Policy and Procedures for Minimum Necessary.
2. The following uses and disclosures of the Plan's PHI for "health care operations" purposes are permitted:
 - Legal review
Cost management
Quality assessment and rating provider and plan performance
Population-based activities
Audits and fraud and abuse detection
Business planning
General administration
 - a. Additional uses and disclosures may also fall within the Privacy Rule's definition of "health care operations." The Privacy Officer will determine on a case-by-case

basis if a particular use or disclosure not listed above is a health care operations activity. If that activity is common or recurring, it shall be added to the list above.

- b. All uses and disclosures of PHI for health care operations activities will comply with the Plan's Policy and Procedures for Minimum Necessary.
3. The Privacy Rule permits other additional uses and disclosures of the Plan's PHI. Those additional uses and disclosures are described in the remainder of these procedures:
- a. To the Plan's service provider business associates (provided a business associate agreement is in place).
 - b. To other covered entities that are members of the Plan's Organized Health Care Arrangement.
 - c. For the treatment and payment activities of another covered entity.
 - i. Upon request by a health care provider, the Plan will disclose PHI to a health care provider for that provider's treatment activities.
 - ii. Upon request by another covered entity or a health care provider, the Plan will disclose PHI for purposes of the requestor's payment activities.
 - iii. The Plan assumes the information requested by a provider or another covered entity is the Minimum Necessary.
 - d. For the following health care operations activities of another covered entity. Upon request by another covered entity, the Plan will disclose PHI for purposes of the requestor's health care operations activities if the following conditions are met:
 - i. The other entity has or had a relationship with the participant or beneficiary who is the subject of the PHI.
 - ii. The health care operation activity is one of the following types of activities:
 - Quality assessment and improvement;
 - Population-based activities relating to improving health or reducing health care costs;
 - Case management;
 - Conducting training programs;
 - Accreditation, certification, licensing, or credentialing; or
 - Health care fraud and abuse detection or compliance.

- iii. The Plan assumes that the information requested by a covered entity is the Minimum Necessary.
- e. As required by law.
 - i. The Plan will use or disclose PHI as required by law.
 - ii. The Privacy Officer will determine on a case-by-case basis whether uses and disclosures are required by law.
 - iii. The Privacy Officer will ensure that uses or disclosures required by law will be limited to the requirements of the law. The Plan's Minimum Necessary policy does not apply to uses or disclosures required by law.
 - iv. The following uses and disclosures required by law have additional requirements, as discussed below in these procedures:
 - Relating to victims of abuse, neglect, or domestic violence;
 - Judicial or administrative proceedings;
 - Disclosures for law enforcement purposes; and
 - Disclosures related to Reproductive Health Care.
- f. For public health activities. Uses or disclosures of PHI for public health activities will be rare. See the Privacy Officer for any uses or disclosures potentially falling within this category.
- g. For health oversight activities. The Plan will disclose PHI for purposes of health oversight activities.
 - i. Health oversight activities are those relating to oversight of:
 - The health care system;
 - Government benefit programs for which health information is relevant to beneficiary eligibility;
 - Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
 - Entities subject to civil rights laws for which health information is necessary for determining compliance.
 - ii. The following are some of the health oversight agencies to whom the Plan may make health oversight disclosures:

- U.S. Department of Labor
Employee Benefits Security
Administration
- EEOC
- Federal offices of inspectors
general
- Department of Justice
- Occupational Health and Safety
Administration
- Defense Criminal Investigative
Services
- Social Security Administration
- HHS Office for Civil Rights
- Food and Drug Administration
- State insurance agencies
- Medicaid fraud control units

- iii. Disclosures will be made under the Plan's policy for disclosures for law enforcement purposes if (a) the use or disclosure relates to a particular individual, and (b) the oversight activity is not directly related to the receipt of health care or qualification for public benefits related to health care.
- iv. For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.
- v. The Plan assumes that information requested by a public official for health oversight activities is the Minimum Necessary.

h. Related to victims of abuse, neglect, or domestic violence.

- i. If the Privacy Officer determines, based on PHI that legitimately came to his or her attention or to the attention of a Plan workforce member, that a participant or beneficiary is the victim of abuse, neglect, or domestic violence, then this information may be disclosed as follows:
 - To a government authority authorized by law to receive reports of abuse, neglect, or domestic violence.
 - The disclosure must be required by another law. The Privacy Officer will consult with legal counsel to ensure that the disclosure is required by law.
 - The Privacy Officer must notify the participant or beneficiary of the disclosure (unless the Privacy Officer determines notification would harm the participant or beneficiary, or if the appropriate disclosure

would be to a personal representative, and it is the personal representative that is causing the abuse, neglect, or harm).

- ii. If the Privacy Officer or other Plan workforce member suspects a participant or beneficiary is the victim of abuse, neglect, or domestic violence, and that suspicion is not based on information in the Plan records, the Privacy Rule and this policy do not apply to any disclosure of those suspicions to the appropriate authorities.
- i. For judicial or administrative proceedings.
 - i. All legal documents seeking PHI for judicial or administrative proceedings immediately should be directed to the Privacy Officer, who will determine the appropriate response based on these procedures, in consultation with legal counsel.
 - ii. Judicial orders and subpoenas. The Plan's PHI may be disclosed pursuant to a judicial order or valid subpoena from a court or an administrative tribunal.
 - The disclosure must be limited to the information expressly authorized in the order or subpoena.
 - The Plan's Policy and Procedures on the Minimum Necessary Standard does not apply to this type of disclosure.
 - iii. Discovery requests and non-judicial subpoenas. If the Plan receives a discovery request or subpoena that is not issued by a court or administrative tribunal, then the Privacy Officer, in consultation with legal counsel, will comply if one of the following conditions is met:
 - The discovery request or subpoena is accompanied by a written statement showing that: (1) the requestor made a good faith attempt to provide written notice to the individual whose PHI is requested; (2) the notice included enough information about the litigation such that the individual could raise an objection to the court/administrative tribunal; and (3) the time for the individual to raise objection has elapsed and no objections were filed or, if filed, have been resolved by the court.
 - The discovery request or subpoena is accompanied by a written statement showing that there is either a stipulated or court issued protective order that prohibits the use or disclosure of the PHI outside the litigation, and requires that the PHI be returned to the covered entity or destroyed at the conclusion of the proceeding.

- If the discovery request or subpoena does not meet the requirements of either statement above, then the Privacy Officer may disclose the requested PHI by ensuring that the above requirements are met (that is, notify the individual as required or obtain a protective order).
- iv. For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.
- j. For law enforcement purposes. The Privacy Officer, in consultation with legal counsel as appropriate, may disclose PHI to a law enforcement official (i.e., someone having authority to investigate potential violations of law, or to prosecute or conduct criminal, civil, or administrative proceedings arising from alleged violations of the law) in the following circumstances:
- i. When the disclosure is required by law.
- ii. Pursuant to a court order, warrant, subpoena, or summons issued by a judicial officer (including a grand jury subpoena).
- iii. Pursuant to an investigative request from an administrative body, but only if the following additional conditions are met:
- The Privacy Officer determines that the information sought is relevant and material to a legitimate law enforcement inquiry;
 - The request is specific and limited in scope in light of the purpose for which the information is sought; and
 - De-identified information cannot reasonably be used.
- iv. To identify or locate an individual, but only if officially requested. The PHI from Plan records that may be disclosed in such circumstances is strictly limited to:
- Name and address
 - Social security number
 - Type of injury
 - A description of distinguishing physical characteristics, including height, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos
 - Date and place of birth
 - ABO blood type and rh factor
 - Date and time of treatment
 - Date and time of death, if applicable

Note: Information in the Plan Sponsor's non-group health plan records is not subject to the Privacy Rule.

- v. About individuals who are suspected to be crime victims, but only if (1) the individual agrees orally or in writing to the disclosure, or (2) if the individual is unable to agree because of incapacity, in which case the Privacy Officer may determine that disclosure is appropriate, but only if the following conditions are met:
 - The law enforcement official states that he or she needs the information to determine whether another person has violated the law (and the information will not be used against the victim);
 - The law enforcement official states that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
 - In the Privacy Officer's professional judgment, the disclosure is in the potential crime victim's best interest.
- vi. About a crime relating to the Plan.
- vii. For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.
- k. About decedents. The Plan will treat any person authorized to act as the personal representative of a participant or beneficiary that is deceased (e.g., an executor or administrator) as though he or she is the participant or beneficiary. The Plan will also disclose a decedent's PHI to a family member or others who were involved in the care or payment for care prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Plan.
- l. To avert a serious threat to health or safety. The Privacy Officer will determine when a disclosure of PHI is necessary to avert a serious threat to health or safety. The following criteria apply to any such disclosure:
 - i. It must not conflict with other applicable law and standards of ethical conduct.
 - ii. It must be based on good faith.
 - iii. It must be necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
 - iv. It must be to a person or to people reasonably able to prevent or lessen the threat, including the target of the threat.
 - v. It must be limited to the following information:

- Name and address
 - Social security number
 - Type of injury
 - A description of distinguishing physical characteristics, including height, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos
 - Date and place of birth
 - ABO blood type and rh factor
 - Date and time of treatment
 - Date and time of death, if applicable
- m. Relating to national security and intelligence activities.
- i. The Privacy Officer will disclose PHI to authorized federal officials for intelligence and other national security activities.
 - ii. Disclosures for national security and intelligence activities are not subject to the Plan's Policy and Procedures on the right to Request an Accounting of Disclosures.
- n. For workers' compensation. The Plan will disclose PHI in compliance with applicable state and federal workers' compensation laws (i.e., any state or federal law that has the effect of providing benefits for work-related injuries or illness without regard to fault).
- o. To the personal representative of participant or beneficiary.
- i. Adult or emancipated minor. The Plan will disclose PHI to an adult or emancipated minor's personal representative to the extent the PHI is relevant to the personal representation.
 - ii. Unemancipated minor. The Plan will disclose PHI to the parent, guardian, or other personal representative of an unemancipated minor only to the extent required, permitted, or prohibited by state law.
 - iii. Exceptions: The Plan will not disclose PHI to the personal representative of a participant or beneficiary if the Privacy Officer reasonably believes, and documents that belief, that:
 - The participant or beneficiary has been or may be abused or neglected by the personal representative;
 - The participant or beneficiary will be endangered if the personal representative relationship is recognized;

- The Plan, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative; or
- The personal representative is making a request related to the provision or facilitation of Reproductive Health Care.

4. The Privacy Rule prohibits or restricts the following uses and disclosures of the Plan's PHI:
- a. Sale of PHI. The Plan will not sell PHI in a manner not permitted by the Privacy Rule without the authorization from any impacted individual.
 - b. Genetic Information. The Plan will not use or disclose genetic information for underwriting purposes.
 - c. Reproductive Health Care Information. The Plan will not use or disclose PHI for any of the following activities:
 - i. to conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care;
 - ii. to impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care; or
 - iii. to identify any person for the purposes described above.

This Reproductive Health Care prohibition applies only when the Plan reasonably determines: (1) the Reproductive Health Care is lawful under applicable state or federal law under the circumstances in which it was provided; or (2) the Reproductive Health Care presumption applies.

B. Disclosures to Plan Sponsor

POLICY:

The Plan may only disclose PHI to the Plan Sponsor under the following conditions: (i) the disclosure is pursuant to a written authorization; (ii) the PHI is limited to Summary Health Information that has been requested by the Plan Sponsor for the purposes of obtaining premium bids, or amending or terminating the Plan; (iii) the PHI is enrollment, disenrollment or participation information; or (iv) the PHI is disclosed for plan administration functions.

PROCEDURES:

1. If the Plan is disclosing PHI for plan administrative functions, the Plan must determine that the Plan Sponsor has satisfied the Plan documentation requirements described in Part I of these policies and procedures.
2. Plan administrative functions must be within the scope of payment or health care operations. Examples include disclosure for administrative review of claims and participant advocacy.

C. Minimum Necessary Standard

POLICY:

The Plan will use or disclose only the Minimum Necessary amount of PHI in order to achieve the purpose of the use or disclosure.

PROCEDURES:

1. The use and disclosure of participant information PHI minimum necessary standard does not apply in the following circumstances:
 - a. The PHI is for use by or a disclosure to a health care provider for treatment purposes;
 - b. The disclosure is to the participant or the participant's legally authorized representative;
 - c. The disclosure is pursuant to a valid authorization, in which case, the disclosure will be limited to the PHI specified on the authorization;
 - d. The disclosure is to the Secretary of Health and Human Services; or
 - e. The disclosure is required by law.
2. The Privacy Officer will make reasonable efforts to limit the access of the Plan's workforce members to their related types of PHI by taking the following steps:
 - a. Each department is responsible for identifying those individuals in the department who need access to PHI in order to carry out their duties and the PHI or types of PHI to which access is needed.
 - b. Each department is responsible for identifying any conditions that would have an impact on a workforce member's ability to access and/or disclose the PHI.
 - c. Each department is responsible for making reasonable efforts to limit the access to PHI to that necessary to carry out the job duties, functions, and/or responsibilities.
3. The departments will implement standard protocols that limit the PHI to uses or disclosures of the amount reasonably necessary to achieve the purpose of the use or disclosure.
4. The Privacy Officer will review non-routine uses and disclosures on a case-by-case basis to determine the Minimum Necessary requirement.
5. When requesting PHI from another covered entity, the Plan must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are made on a routine and recurring basis the Plan shall take

reasonable steps to ensure that the request is limited to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.

6. The Privacy Officer need not make a determination of Minimum Necessary in the following situations (and can, instead, assume that the requestor's statement of information needed is the Minimum Necessary):
 - a. A public official when the disclosure is one that is permitted pursuant to the Plan's use and disclosure policy (pursuant to law, for health oversight purposes, etc.);
 - b. Covered Entities;
 - c. An employee if the individual represents that the information requested is the minimum necessary for the stated purpose; and
 - d. The Plan's service provider business associates, as long as the disclosure is for the purposes of carrying out the services under the service provider contract.

D. Written Authorizations

POLICY:

The Plan will obtain written authorizations for the use or disclosure of PHI not permitted under the Privacy Rule. The Plan will disclose PHI upon the request of another entity upon receiving a valid authorization. The Plan does not condition eligibility for enrollment in, or coverage under the Plan on, the receipt of any authorization from a participant or beneficiary.

PROCEDURES:

1. Written authorizations must be obtained from participants and beneficiaries before making the following uses or disclosures of their PHI:
 - a. any PHI use or disclosure that this privacy policy does not specifically require or permit;
 - b. any communications for marketing purposes, unless an exception is provided for in the HIPAA Rules; or
 - c. any use or disclosure of psychotherapy notes.
2. Content of authorizations. The Plan will use its standard Authorization form for all authorizations except those initiated by other entities.
 - a. Authorizations should be modified to specifically state the PHI to be used or disclosed, to whom it will be disclosed, and the purpose of the disclosure.
 - b. The Privacy Officer will review each authorization or type of authorization to ensure it meets the requirements of the Privacy Rule.
 - c. Multiple authorizations may be combined for uses or disclosures of PHI, except that an authorization may not be combined with any non-authorization document or with an authorization for the use or disclosure of psychotherapy notes.
3. Revocations. The Plan will honor all written revocations of authorization.
 - a. All revocations should be sent to the Privacy Contact, who will forward them to the Privacy Officer.
 - b. The Privacy Officer will ensure that uses and disclosures previously authorized cease.
4. Refusal to sign an authorization does not affect a participant's or beneficiary's rights relating to eligibility for, enrollment in, or coverage under the Plan.
5. Authorizations initiated by participants, beneficiaries, or other entities.

- a. The Plan may receive a request for information from another entity or a request from a participant or beneficiary to disclose his or her PHI to another entity.
 - b. The Privacy Officer must review all authorizations received from participants, beneficiaries, or other entities to ensure that the authorizations meet the requirements of the Privacy Rule. Disclosures will not be made if the authorizations are not sufficient under the Privacy Rule.
6. The Plan's minimum disclosure policy does not apply to uses or disclosures made pursuant to an authorization. The PHI used or disclosed will be consistent with the information authorized to be used or disclosed.
7. Documentation. Signed authorization forms and revocations will be maintained by the Plan for six years following the date last in effect.

E. Oral or Implicit Permission to Disclose PHI

POLICY:

The Plan will disclose PHI to a person who is involved in a participant's or beneficiary's health care or payment related to that health care when the participant or beneficiary orally or implicitly permits such a disclosure (as governed by the Privacy Rule). Such disclosures that are requested when the participant or beneficiary is not present will only be made to a member of the participant's or beneficiary's immediate family.

PROCEDURES:

1. This policy applies to inquiries by a family member or friend about a participant's or beneficiary's status or benefits. This policy does not apply to inquiries by family members who are the personal representative of another family member. Personal representatives are generally treated as the participant or beneficiary.
2. Phone or in person – participant or beneficiary present.
 - a. If an individual contacts the Plan Sponsor regarding a participant's or beneficiary's status or benefits, the Employee Benefits Representative should in all cases try to obtain oral agreement from the participant or beneficiary before communicating with the individual.
 - i. If the inquiry is in person, and the participant or beneficiary is present, obtain his or her verbal agreement that PHI may be shared with the inquiring individual.
 - ii. If the inquiry is by phone, ask to speak with the participant or beneficiary, if he or she is available, and obtain his or her verbal agreement that PHI may be shared with the inquiring individual.
 - b. Once verbal agreement is obtained, the Employee Benefits Representative may disclose the following categories of information:
 - i. Confirm eligibility or enrollment information;
 - ii. Provide general information regarding healthcare plan provisions; and
 - iii. Provide assistance with claims resolution.
 - c. Suggest to the participant or beneficiary that he or she may wish to give the Plan written authorization to disclose PHI to certain family members or friends involved in the participant's or beneficiary's health care. See the Plan's policy on authorizations.

3. Phone, in person, or by correspondence (including e-mail) – participant or beneficiary not present.
 - a. If a member of the participant's or beneficiary's immediate family contacts the Plan Sponsor regarding a participant's or beneficiary's status or benefits and the participant or beneficiary is not present at the time an inquiry is made on his or her behalf, the Employee Benefits Representative should:
 - i. Verify the identity of the individual and his or her immediate family relationship to the participant or beneficiary.
 - ii. Review the participant's or beneficiary's records to ensure that there is no restriction or confidential communication request in place. (If there is, the Employee Benefits Representative should not disclose any PHI to the individual.)
 - b. The Employee Benefits Representative should determine if the disclosure requested is in the best interests of the participant or beneficiary. If so, the disclosure should be limited as follows:
 - i. Confirm eligibility or enrollment information;
 - ii. Provide general information regarding healthcare plan provisions; and
 - iii. Provide assistance with claims resolution.
 - c. The PHI disclosed must be limited to that directly relevant to the inquiring individual's involvement in the participant's or beneficiary's health care.

F. Disclosures Requiring Attestation

POLICY:

The Plan will obtain an attestation for any request of PHI that is potentially related to Reproductive Health Care if the request is made for disclosures for health oversight activities, disclosures for judicial and administrative proceedings, disclosures for law enforcement purposes, disclosures required by law, or disclosures about decedents to coroners and medical examiners. If the Plan, upon receipt of the attestation and additional investigation, determines that the request is not for purposes of investigating or imposing liability for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care that was lawful under the circumstances in which it was provided, the Plan may disclose the PHI upon the request.

PROCEDURES:

1. The Plan will presume Reproductive Health Care is lawful under the circumstances in which such health care is provided unless the Plan has:
 - a. Actual knowledge that the Reproductive Health Care was not lawful under the circumstances in which it was provided; or
 - b. Factual information supplied by the person requesting the use or disclosure of PHI that would demonstrate to a reasonable covered entity a substantial factual basis that the Reproductive Health Care was not lawful under the specific circumstances in which such health care was provided.
2. All requests for PHI related to Reproductive Health Care for purposes as stated above must be accompanied by a valid attestation. A valid attestation for these purposes is a document that must only contain the following elements:
 - a. A description of the information requested that identifies the information in a specific fashion, including one of the following:
 - i. The name of any individual(s) whose PHI is sought, if practicable; or
 - ii. If including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose PHI is sought.
 - b. The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure;

- c. The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure;
 - d. A clear statement that the use or disclosure is not for a purpose prohibited under the Privacy Rule;
 - e. A statement that a person may be subject to criminal penalties if that person knowingly and in violation of HIPAA obtains Individually Identifiable Health Information relating to an individual or discloses Individually Identifiable Health Information to another person; and
 - f. Signature of the person requesting the PHI, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.
3. An attestation is not valid and, therefore will not be accepted by the Plan if the document submitted has any of the following defects:
 - a. The attestation lacks an element or statement required by the list as stated above;
 - b. The attestation contains an element or statement not required by paragraph 2 of this section;
 - c. The attestation is combined with any other document except where such other document is needed to satisfy the requirements of this Section of the Policies or other sections of the Privacy Rule as applicable;
 - d. The Plan or its business associate has actual knowledge that material information in the attestation is false; or
 - e. In light of the facts and circumstances of the request, a reasonable covered entity or Business Associate in the same position as the Plan would not believe that the attestation is true.
4. The Plan will only accept an attestation that has been written in plain language that clearly identifies the purpose of the request.
5. If, during the course of using or disclosing PHI in reasonable reliance on a facially valid attestation, the Plan or its Business Associate discovers information reasonably showing that any representation made in the attestation was materially false, leading to a use or

disclosure for a purpose prohibited under the Privacy Rule, the Plan or its Business Associate will cease such use or disclosure.

G. De-Identified Information

POLICY:

The Plan will use or disclose de-identified information instead of PHI to the extent practicable.

PROCEDURES:

1. The following common and recurring uses and disclosure by the Plan of health information will be conducted using de-identified information: (i) plan utilization and cost; (ii) plan design; (iii) participation in healthcare surveys; (iv) reporting required by government agencies; and (v) joint Managed Care Committee operations
2. The Privacy Officer will review other uses and disclosures on a case-by-case basis to determine if de-identified information is preferable to PHI.
3. The Privacy Officer will work with the Plan's third-party administrator, insurer, or HMO to obtain the relevant PHI for purposes of creating de-identified information.
4. If necessary, the Privacy Officer will engage a service provider to create the de-identified information. Any such service provider will sign a business associate agreement as required under the Plan's Policy and Procedures for Business Associates.
5. The Privacy Officer will ensure that none of the following data elements are included in any de-identified information (or alternatively, will engage a statistical expert to determine that the risk of identifying an individual based on the information included is very small):

- Names
- All geographic units smaller than a state (except for the first three zip code digits if the number of persons in that zip code region is greater than 20,000)
- All ages over 89
- Internet Protocol address numbers
- Medical record numbers
- Account numbers
- Vehicle identifiers and serial numbers (including license plate numbers)
- Full face photos (and comparable images)
- All dates (except year)
- Telephone and fax numbers
- Social security numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Device identifiers and serial numbers
- E-mail addresses
- URLs
- Biometric identifiers (including finger and voice prints)
- Any other unique identifying number, characteristic, or code

H. Requests for Restrictions on Use or Disclosure of PHI

POLICY:

Participants or beneficiaries have the right to request that the Plan (a) restrict using or disclosing PHI for payment and health care operations, and (b) restrict disclosing PHI to family members or friends involved in their care or payment relating to their care. The Plan *will not* agree to restrictions on its use and disclosure of PHI relating to payment and health care operations. The Plan generally *will* accommodate requests to restrict disclosures to family members or friends involved in the care or payment of care of the participant or beneficiary, provided those restrictions are administratively feasible.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this policy. All questions should be addressed, in the first instance, by the Privacy Officer.
2. Participants and beneficiaries must request restrictions on the use and disclosure of their PHI in writing. In general, before responding to such a request, the Employee Benefits Representative should review it for completeness. It should contain the following information:
 - a. Name, address, and daytime phone number of the participant or beneficiary making the request; and either:
 - b. The manner in which the participant or beneficiary wishes the Plan to restrict its uses and disclosures of PHI for payment and health care operations; or
 - c. The persons involved in their care to whom the Plan should not disclose PHI.
3. If a participant or beneficiary requests a restriction on the use or disclosure of PHI for payment and health care operations purposes, in almost all instances the Employee Benefits Representative should send a response stating that the request has been denied.
4. If the participant or beneficiary has requested that the Plan not disclose his or her PHI to certain family members or friends, the Employee Benefits Representative should take the following steps:
 - a. Determine whether the requested restriction is feasible. This may include discussing the restriction with service providers (such as the Plan's third party administrator).
 - b. If the restriction is feasible, send a written response indicating that the Plan agrees to the restriction. Inform relevant service providers (such as the Plan's third-party administrator) of the restriction.

- c. Consider whether the participant or beneficiary intended to request confidential communications of PHI. These are generally granted if reasonable, and if the participant or beneficiary alleges that he or she will be subject to harm if the PHI is disclosed. See the Plan's Policy and Procedures on Requests for Confidential Communications.
 - d. If the restriction is not feasible, send a response stating that the request has been denied.
5. The Employee Benefits Representative should ensure that agreed-to restrictions are communicated to relevant service provider business associates.
6. If the Plan determines it no longer wishes to continue operating in accordance with an agreed-to restriction, it may terminate the restriction by:
- a. Obtaining oral or written assent from the participant or beneficiary.
 - i. Assent should be documented.
 - ii. If the participant or beneficiary agrees, then the restriction is terminated both prospectively and retrospectively.
 - b. Notify the participant or beneficiary that the agreed-to restriction is terminated.
 - i. This method of terminating an agreed-to restriction should be used only if the Employee Benefits Representative is unable to obtain oral or written assent from the participant or beneficiary.
 - ii. A restriction terminated by notification operates prospectively only.
7. If the participant or beneficiary notifies the Plan that he or she no longer needs the restriction, the restriction will be lifted both prospectively and retrospectively.
8. All written requests for privacy protection must be tracked on the Privacy Protection Request Tracking Log.
9. All written requests for privacy protection to which the Plan has agreed, and any termination documentation, must be maintained by the Plan for six years from the date the document was created or the date it was last in effect, whichever is later.

I. Requests for Confidential Communications

POLICY:

Participants and beneficiaries have the right to request that communications to them about their PHI be by alternative means or alternative locations. The Plan will agree to requests for confidential communications but only if (1) the requestor states that disclosure of the information at issue could endanger him or her; (2) the request is in writing; and (3) the alternative means or alternative locations given for the communications are administratively reasonable.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this policy. All questions should be addressed, in the first instance, by the Privacy Officer.
2. Participants and beneficiaries who wish to request confidential communications must do so in writing. In general, before responding to such a request, the Employee Benefits Representative should review it for completeness. It should contain the following information:
 - a. Name, address, and daytime telephone number of the participant or beneficiary making the request;
 - b. The types or categories of communications to which the request applies;
 - c. The alternative means or locations for the Plan to continue the communications with the participant or beneficiary; and
 - d. A statement that the participant or beneficiary believes that the disclosure of PHI in the identified communications could endanger him or her.
3. The Employee Benefits Representative should deny the request in writing if it does not include a statement that the participant or beneficiary fears he or she will be endangered.
4. The Employee Benefits Representative should deny the request in writing if the requested alternative means or location is not feasible. Investigate whether the alternative means or location is feasible, including conducting discussions with relevant service providers, such as its third-party administrator.
5. Granting a request.
 - a. If the request is feasible, or partially feasible, the Employee Benefits Representative should send a written response that includes a statement describing what communications are covered and the manner in which they will be communicated.

- b. Consider whether, even if it is feasible, there might be other ways the information will be disclosed to someone who could endanger the participant or beneficiary. Example: Explanations of Benefits (EOBs) relating to a beneficiary dependent's reproductive health medical services can feasibly be sent to a Post Office box separate from her home address. It may be, however, that later EOBs sent to the participant will include an indication that part of the covered charge for the beneficiary's services qualified toward the deductible. If such a situation exists, carefully explain it in the response.
 - c. Inform relevant service providers (such as the Plan's third-party administrator) of any agreed-to confidential communication.
6. All written requests for privacy protection must be tracked on a log of privacy protection requests.
7. All written requests for confidential communication to which the Plan has agreed must be maintained by the Plan for six years from the date the document was created or the date it was last in effect, whichever is later.

J. Right of Access to PHI

POLICY:

Beneficiaries and participants, or their personal representatives, have a right to access PHI contained in the Plan's designated record sets. The Plan's designated record sets include: (i) dependent status and data (ii) Medicare eligibility; (iii) other insurance; (iv) claims history; (v) coverage history; (vi) treatment history; (vii) treating provider; (viii) primary care physician; (ix) health Plan election; (x) diagnosis; (xi) treatment code; and (xii) cost of coverage.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this policy. All questions should be addressed, in the first instance, by the Privacy Officer.
2. Participants and beneficiaries, or their personal representatives, must request access to their PHI in writing. In general, before responding to such a request, the Employee Benefits Representative should review it for completeness. It should contain the following information:
 - a. Name, address, and daytime telephone number of the participant or beneficiary making the request;
 - b. If submitted by personal representative, proof of status;
 - c. Time period of the request; and
 - d. Form of access requested (on-site, mailed copy, etc.).
3. Requests for access must be granted or denied within 30 days from the date a written request is received. If you need more time, send a notice indicating that additional time (up to an additional 30 days) is needed to respond to the access request.
4. If the PHI requested is maintained electronically in one or more designated record sets, and the participant or beneficiary requests an electronic copy of such information, the Plan will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format. If the PHI is not readily producible in such form and format, the PHI will be produced in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual cannot agree on an acceptable electronic form and format, the Plan will provide a paper copy of the information.
5. Reviewing a Request.
 - a. Determine whether any requested PHI is in a designated record set and if the information is maintained electronically (if requested).

- b. Determine if there is any basis on which to deny or partially deny the request. The following are permissible bases for denial:
 - i. If the request is made by a person asserting that he or she is the personal representative of a participant or beneficiary, review the documentation provided to verify that status. If the documentation is inadequate, or if the requested information is not within the scope of the personal representation, deny the request.
 - ii. The Privacy Officer, after consulting with a licensed health care professional, determines that access will endanger the life or physical safety of the participant or beneficiary or another person.
 - iii. The requested PHI contains psychotherapy notes.
 - iv. The requested PHI was compiled by the Plan or one of its business associate service providers in anticipation of a legal proceeding.
 - v. The information was obtained from someone other than a covered health care provider under a promise of confidentiality and access would likely reveal the source of the information.
- c. If a denial is appropriate, send a written notice denying the request for access. Provide partial access if possible.
- d. Granting a Request.
 - i. Gather the PHI from designated record sets. If copies are to be provided, keep track of the time spent copying the records and the cost of the copies.
 - ii. Send the Response to Request for Access to the requestor.
 - Provide the access or information in the manner requested, if possible; or
 - If not possible, contact requestor to reach an agreement on an alternative manner of delivery (for example, on-site inspection).
6. If the participant, beneficiary, or personal representative appeals a denial that was based on "safety" concerns, the appeal will be reviewed, after consulting with a different licensed health care professional, who should determine within a reasonable period of time whether the denial was appropriate. No other basis for denial is appealable.
7. All documents received or sent relating to the right of access must be tracked on a log of access requests.
8. All written requests, responses, or other related correspondence must be maintained by the Plan.

K. Right to Request Amendment of PHI

POLICY:

Beneficiaries and participants, or their personal representatives, have a right to request amendment of their PHI contained in the Plan's designated record sets. The Plan's designated record sets include: (i) dependent status and data (ii) Medicare eligibility; (iii) other insurance; (iv) claims history; (v) coverage history; (vi) treatment history; (vii) treating provider; (viii) primary care physician; (ix) health Plan election; (x) diagnosis; (xi) treatment code; and (xii) cost of coverage.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this policy. All questions should be addressed, in the first instance, by the Privacy Officer.
2. Participants and beneficiaries, or their personal representatives, must submit amendment requests in writing.
 - a. In general, before responding to the request, the Employee Benefits Representative should ensure it has the following information:
 - i. Name, address, daytime telephone number of the participant or beneficiary making the request;
 - ii. If submitted by personal representative, proof of status;
 - iii. The particular PHI requested to be amended; and
 - iv. Specific reasons for the requested amendment (i.e., a statement of why the existing PHI is inaccurate or incomplete).
 - b. No response is required if an amendment request is not submitted in writing and does not contain the reasons supporting the proposed amendment.
3. Amendment requests must be granted or denied within 60 days from the date the written request is received. If it is not possible to respond to an amendment request within 60 days from the date of the request, the Plan may, upon notice to the requestor, take an additional 30 days. The notice of additional time in which to respond must be sent within 60 days from the date of the original amendment request.
4. Denying an amendment request.
 - a. An amendment request may be denied if:
 - i. The Privacy Officer determines the existing PHI is accurate and complete.

- ii. The PHI was not created by the Plan (unless the requestor establishes that the originator of the PHI no longer is available to act on the request).
 - iii. The PHI is not in the Plan's designated record sets.
 - iv. The information would not be subject to the right of access, meaning it falls into one of the following four categories:
 - The Privacy Officer, after consulting with a licensed health care professional, determines that access will endanger the life or physical safety of the participant or beneficiary or another person.
 - The requested PHI contains psychotherapy notes.
 - The requested PHI was compiled by the Plan or one of its business associates in anticipation of a legal proceeding.
 - The information was obtained from someone other than a covered health care provider under a promise of confidentiality and access would likely reveal the source of the information.
 - b. If a denial of the amendment request is appropriate, send a written notice denying the request for amendment.
5. Participants and beneficiaries may not appeal a denial of their amendment requests. Instead, they may take, and the Plan Sponsor will respond to, the following actions:
 - a. Written statement of disagreement. Participants and beneficiaries may submit a written statement of disagreement of no more than one page.
 - i. If the Privacy Officer determines it is necessary, a rebuttal to the written statement of disagreement may be prepared.
 - ii. The written statement of disagreement (and rebuttal, if any) will be appended or linked to the PHI that is the subject of the amendment request.
 - iii. The written statement of disagreement (and rebuttal, if any) will be disclosed with any subsequent disclosure of the PHI that is the subject of the amendment request.
 - b. Request to include amendment request and denial when disclosing information. A participant or beneficiary may request that their original amendment request and the Plan's denial be disclosed with subsequent disclosures of the PHI that is the subject of the amendment request. Such a request must be complied with.
6. Granting a request.

- a. Identify the records in the designated record sets that contain the PHI that is the subject of the amendment request. The PHI may be maintained by the Plan's service providers.
 - b. Append or link the amendment to the relevant PHI records.
 - c. Notify the requestor in writing that the Plan is granting the request. If the requestor submits the names of persons or entities who he or she believes have received the medical or health information that is the subject of the amendment request, share the amendment with those persons or entities.
 - d. Inform persons or entities, such as service providers, that may have relied on the PHI that is the subject of the request.
7. Notices from other covered entities of amendments to PHI. Upon receipt of a notice from another covered entity that the covered entity has agreed to the amendment request of a participant or beneficiary, append or link the amendment in the relevant records in the Plan's designated record sets.
 8. All documents received or sent relating to amendment requests must be tracked on a log of amendment requests.
 9. All written requests, responses, or other related correspondence relating to amendment requests must be maintained by the Plan.

L. Right to Request an Accounting of Disclosures

POLICY:

Participants and beneficiaries, or their personal representatives, have a right to request an accounting of certain disclosures of their PHI made by the Plan. They are entitled to one free accounting within a twelve-month period. The Plan charges reasonable actual costs for any additional requests within a twelve-month period.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this policy. All questions about accountings should be addressed, in the first instance, by the Privacy Officer.
2. The following disclosures (and responsible department acting for the group health plan) must be recorded whenever they occur to ensure that the Plan will be able to respond to requests from participants and beneficiaries for an accounting of disclosures.

<u>Type of Disclosure</u>	<u>Name of Responsible Department acting for the Plan or Business Associate(s), if any</u>
Disclosures required by law Judicial and administrative proceedings disclosures Disclosures for law enforcement purposes	Employee Benefits Department Legal Department
Public health activities disclosures Disclosures to avert a serious threat to health and safety	Employee Benefits Department
Health oversight activities disclosures Disclosures about decedents Disclosures to personal representative or participant or beneficiary	Employee Benefits Department All insurance carriers
Disclosures about victims of abuse, neglect, or domestic violence Disclosures for Workers' Compensation	Employee Benefits Department All insurance carriers

3. Participants and beneficiaries, or their personal representatives, must request an accounting of disclosures of their PHI in writing. In general, before responding to the request, the Employee Benefits Representative should ensure the request includes the following information:
 - a. Name, address, daytime telephone number, group health plan enrollment information (i.e., particular plan(s) in which participant or beneficiary is enrolled);
 - b. If submitted by personal representative, proof of status; and
 - c. Time period of the request.
4. The Plan responds to accounting requests within 60 days from the date a written request is received. If the Plan needs additional time to respond, it will send a Notification of Additional Time to Respond to Accounting Request, which entitles the Plan to an additional 30 days in which to respond.
5. Responding to the Request.
 - a. Determine if the requestor has submitted an accounting request in the prior 12 months. If so:
 - i. Send a written notification of the charges for second request in a 12-month period.
 - ii. Do not respond to the accounting request unless you receive an acknowledgment from the requestor agreeing to pay the costs of the accounting.
 - b. If the request has been submitted by a personal representative, review and substantiate personal representative status. Ensure participant or beneficiary has not requested (and been granted) a restriction on disclosures of confidential communications (see the Plan's Policy and Procedures on Requests for Restrictions on Use or Disclosure of PHI and the Plan's Policy and Procedures on Requests for Confidential Communications).
 - c. Request from any plan sponsor workforce member responsible for tracking covered disclosures any covered disclosures within the applicable time frame of the request (no more than six years).
 - d. Request from all relevant business associate service providers any covered disclosures within the applicable time frame of the request.
 - e. Provide an accounting of disclosures.
6. All documents received or sent relating to the right to request an accounting must be tracked on a log of accounting requests.

7. Documentation of all covered disclosures will be maintained by the Plan.
8. All written requests for accountings, responses to such requests, and other related correspondence will be maintained by the Plan.

M. Sanctions for Violating the Privacy Rule

POLICY:

The Plan will sanction any employee that uses or discloses a participant's or beneficiary's PHI in violation of the Plan's privacy policies and procedures or in violation of the Privacy Rule.

PROCEDURES:

1. The Privacy Officer has responsibility for implementation of this policy.
2. All uses and disclosures of PHI that potentially violate the Plan's privacy practices or procedures should be reported directly to the Privacy Officer.
3. The Privacy Officer should, in the first instance, determine whether the allegedly improper use or disclosure violates the Plan's policies and procedures or the Privacy Rule.
4. If there was a violation, the Privacy Officer should take the following steps:
 - a. Determine if the improper use or disclosure was intentional or unintentional;
 - b. Determine if the improper use or disclosure was a one-time incident or constitutes a pattern or practice;
 - c. Determine if there are any mitigating factors (such as self-reporting or lack of proper training or supervision); and
 - d. Based on the results of the Privacy Officer's investigation, the employee or employees who improperly used or disclosed the PHI will be subject to disciplinary action in accordance with appropriate appointing authority's policy, up to and including discharge.
5. The Privacy Officer should consider, in light of the nature of the improper use or disclosure of PHI, if additional training should occur for one or more employees.
6. The Privacy Officer should consider, in light of the nature of the improper use or disclosure of PHI, whether any of the Plan's policies or procedures need to be amended.
7. The Privacy Officer or his/her designee will maintain records showing the sanctions imposed under this policy for six years following the date the sanctions are imposed. These documents will be maintained by the Plan.

N. Privacy Complaints

POLICY:

The Privacy Officer will receive and respond to all complaints about the Plan's privacy policies, its adherence to those policies, or its compliance with the Privacy Rule.

PROCEDURES:

1. The Privacy Officer has responsibility for implementation of this policy. If the Privacy Contact and the Privacy Officer are different, the Privacy Contact will forward all complaints to the Privacy Officer.
2. Upon receiving a complaint regarding the Plan's privacy policies, its adherence to those policies, or its compliance with the Privacy Rule, the Privacy Officer will investigate and, with the assistance of legal counsel if necessary, determine if there is any validity to the complaint.
 - a. If the complaint is not valid, meaning the Plan has not violated its policies and procedures or the Privacy Rule, then the Privacy Officer will send an appropriate response to the individual who submitted the complaint.
 - b. If the Privacy Officer determines that the complaint is valid, the following steps will be taken:
 - i. If the complaint is that the Plan's privacy notice, as written, does not comply with the Privacy Rule, and the complaint does not allege any improper use or disclosure of PHI, then the Privacy Officer will determine whether an amendment of the privacy notice (and of the Plan's policies and procedures) is necessary to correct the alleged violation.
 - ii. If the complaint is that the Plan or one of its service providers used or disclosed PHI in a way that violates the Plan's privacy policies and procedures or the Privacy Rule, then the Privacy Officer will:
 - Send a letter explaining what steps will be taken to correct any future improper uses or disclosures;
 - Determine whether there is any harm that should be mitigated, if practicable, under the Plan's Policies and Procedures on Mitigation of Harm Due to Improper Uses and Disclosures;
 - If the use or disclosure was by a member of the Plan's workforce, consider whether sanctions should be imposed under the Plan's Policies and Procedures on Sanctions for Violating the Privacy Rule;

- If the use or disclosure was by a service provider, determine whether further investigation or actions are necessary to ensure future violations do not occur;
 - Consider, in light of the nature of the improper use or disclosure of PHI, if additional training should occur for one or more employees; and
 - Consider, in light of the nature of the improper use or disclosure of PHI, whether any of the Plan's policies or procedures need to be amended.
3. All complaints and their disposition (i.e., response letters) must be documented and retained for six years. These documents will be maintained by the Plan.

O. Mitigation of Harm Due to Improper Uses or Disclosures

POLICY:

The Plan will mitigate, to the extent practicable, any harm caused by a use or disclosure of a participant's or beneficiary's PHI that is in violation of the Plan's privacy policies and procedures or in violation of the Privacy Rule.

PROCEDURES:

1. The Privacy Officer has responsibility for implementation of this policy.
2. Upon learning of an improper use or disclosure by a plan sponsor workforce member or service provider, the Privacy Officer will take the following steps:
 - a. Determine whether a participant or beneficiary could be or has been harmed by the improper use or disclosure;
 - b. Determine whether there are any practicable steps that might have a mitigating effect with regard to the potential harm identified; and
 - c. If so, implement the mitigating steps.
 - d. Determine if improper use or disclosure constitutes a Breach. If so, implement the Plan's Breach Policy.

P. No Retaliation or Intimidation

POLICY:

The Plan will not retaliate against any participant or beneficiary who chooses to exercise his or her individual privacy rights, including the right to access PHI, the right to request amendment of PHI, the right to an accounting of disclosures, and the right to request certain privacy restrictions. The Plan also will not intimidate any participant or beneficiary who seeks to exercise those rights. Further, the Plan will not retaliate against or intimidate any person or organization that files a complaint regarding the Plan's privacy practices with HHS, that participates in any investigation of the Plan's privacy practices, or that opposes any act of the Plan that allegedly violates the Privacy Rule.

Q. No Waiver of Rights

POLICY:

The Plan will not require participants or beneficiaries to waive any rights under the Privacy Rule in order to enroll in the Plan or in order to receive the provision or payment of benefits under the Plan.

R. Notice of Privacy Practices

POLICY:

The Privacy Officer is responsible for developing and maintaining a Notice of Privacy Practices that complies with the Privacy Rule.

PROCEDURES:

1. The Notice of Privacy Practices will be provided to each newly eligible employee upon hire, or if later, when the employee first enrolls in the Plan.
2. The Notice of Privacy Practices will be provided to any participant or beneficiary upon request.
3. A new Notice of Privacy Practices will be provided within 60 days of any material revision to these Privacy Policies and Procedures.
4. At least once every three years, the Plan will notify individuals then covered by the Plan of the availability of the Notice of Privacy Practices and how to obtain it.

PART III

SECURITY POLICIES

A. Risk Analysis

POLICY:

The Privacy and Security Officers will periodically conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to the confidentiality, availability and integrity of all Electronic PHI that the Plan or Plan Sponsor creates, receives, maintains, or transmits.

PROCEDURES:

The risk analysis will include the following:

1. A thorough analysis of information systems, including hardware, software, input and output sources, and identification of all Electronic PHI;
2. Identification of possible threats to the confidentiality, integrity, and availability of Electronic PHI. These threats include:
 - a. natural threats such as floods, earthquakes, tornadoes, and landslides;
 - b. human threats such as network and computer based attacks, malicious software upload, unauthorized access to Electronic PHI and unintentional actions (e.g., inadvertent data entry or deletion and inaccurate data entry);
 - c. environmental threats such as power failures, pollution, chemicals, and liquid leakage;
3. Identification of vulnerabilities, such as failure to disable the passwords of terminated employees, poor or nonexistent firewalls, ineffective barriers to viruses and other malicious software, failure to install operation system patches, fire-control measures that damage hardware and software, etc.;
4. Determination of the likelihood and impact of each identified threat; and
5. Identification of the features that should be implemented to lessen threats to a reasonable and appropriate level.

B. Risk Management

POLICY:

The Plan will manage risks to its Electronic PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level. Security measures put into place will be commensurate with the risks to the information systems that store, process, transmit or receive Electronic PHI, and will be designed to reduce the risks to Electronic PHI to reasonable and manageable levels. The risk management plan and these Policies were developed with the understanding that the Plan Sponsor maintains very little Electronic PHI on its systems.

PROCEDURES:

1. To the extent that the Plan Sponsor maintains any applicable security policies or procedures, the Plan will apply these standard policies and procedures to reduce risks and vulnerabilities to a reasonable and appropriate level. To the extent that the existing security policies and procedures do not adequately reduce risks and vulnerabilities to Electronic PHI, the Plan will implement additional measures to reduce the risks and vulnerabilities.
2. The Plan will prioritize risk mitigation efforts based on the following when managing its risks:
 - a. The size, complexity, and capabilities of the Plan;
 - b. The Plan's technical infrastructure, hardware, software, and security capabilities;
 - c. The costs of security measures; and,
 - d. The criticality of the Electronic PHI potentially affected.
3. The Plan will use a risk matrix to assist in determining risk levels and show the likelihood of threat occurrence and resulting impact of threat occurrence.
4. The Plan will prioritize risks using information from the risk analysis. When deciding what resources should be allocated to identified risks, the highest priority will be given to risks with unacceptable risk ratings.

C. Sanctions for Violating the Security Rule

POLICY:

The Plan will sanction any employee that has violated any part of these Policies related to security or the Security Rule.

PROCEDURES:

1. The Appointing Authority or its designee has responsibility for implementation of this Policy.
2. Any incidents that potentially violate the Plan's security practices or procedures should be reported directly to the Appointing Authority.
3. The Appointing Authority should, in the first instance, determine whether the alleged incident violates the Plan's Policies or the Security Rule.
4. If the violation was the result of an act or omission of a workforce member, the Appointing Authority should take the following steps:
 - a. Coordinate with the Privacy Officer to determine if the violation was intentional or unintentional;
 - b. Determine if the workforce member's action or omission was a one-time incident or constitutes a pattern or practice;
 - c. Coordinate with the Plan Sponsor to determine if there are any mitigating factors (such as self-reporting or lack of proper training or supervision); and
 - d. Based on the results of the investigation, the employee or employees involved will be subject to disciplinary action in accordance with Plan Sponsor's policy, up to and including termination.
5. If the violation was the result of an act or omission of a Business Associate or the agent or subcontractor of a Business Associate, the Appointing Authority should take the steps outlined in the Business Associate Agreement and determine if the contractual relationship with the Business Associate should be terminated.
6. The Appointing Authority should coordinate with the Privacy Officer to determine whether the violation resulted in an improper use or disclosure of PHI that could harm the participant or beneficiary or if the violation constituted a breach. If harm may occur, the Privacy Officer should implement the Plan's Policy and Procedures on Mitigation of Harm Due to Improper Uses and Disclosures. If the violation was a breach, the Appointing Authority should implement the Plan's Policy and Procedures on Breach Notifications.

7. The Appointing Authority should consider, in light of the nature of the violation, if additional training should occur for one or more employees.
8. The Appointing Authority should consider, in light of the nature of the security violation, whether any of the Plan's policies or procedures need to be amended.
9. The Appointing Authority or its designee will maintain records showing the sanctions imposed under this Policy for six years following the date the sanctions are imposed. These documents will be maintained by the Plan.

D. User Access Management

POLICY:

The Plan Sponsor shall establish rules for authorizing access to the computing network, applications, workstations, and to areas where Electronic PHI is accessible. Workforce members shall have authorization when working with Electronic PHI or when working in locations where it resides. Workforce security includes ensuring that only workforce members who require access to Electronic PHI for work related activities shall be granted access and that when work activities no longer require access, authorization shall be terminated. The policy also permits management to grant emergency access to workforce members who have not completed HIPAA security training if the facility declares an emergency. In addition, this Policy provides guidelines on how user access is routinely reviewed and updated.

PROCEDURES:

1. The Plan Sponsor will have the responsibility for authorizing all individuals access to the electronic communication systems that contain PHI and the Security Officer or his/her designee will have the responsibility for granting access authority to all individuals authorized by the Plan Sponsor to access to the electronic communication systems that contain PHI.
 - a. Only individuals who have a "need to know" will be provided access to PHI.
 - b. Workforce members will only be granted access to the minimum necessary electronic PHI that they require to perform their duties.
2. Human Resources will, where appropriate, obtain a background check before a person is granted access to PHI.
3. All workforce members with access to Electronic PHI will have a unique identification and password for the electronic systems.
4. All workforce members with access to Electronic PHI through outside vendor websites are given unique identification and passwords to those systems where available.
5. The Security Officer shall maintain an updated list of authorized individuals and their level of access to both internal systems containing PHI and outside vendor systems containing PHI, based on notifications outlined in this Policy.
6. The Plan Sponsor will determine when a workforce member is hired or promoted what level of access the individual will have to the Plan Sponsor's electronic communication system and the data that the workforce member can access and use. The Plan Sponsor will communicate this information to the Security Officer or his/her designee, so that appropriate access is granted.

7. The Plan Sponsor will notify the Security Officer or his/her designee when a workforce member's access needs to be terminated. Within twenty-four (24) hours of such notification, the Security Officer or his/her designee shall terminate access to information systems, including terminating any login capabilities to any systems that contain Electronic PHI, and other sources of PHI including access to rooms or buildings where PHI is located, when a workforce member, agent or business associate ends his or her employment or engagement.
8. Upon notification, the Security Officer or his/her designee will terminate access to specific types of PHI when the status of a workforce member no longer has a "need to know" of those types of information.
9. The Security Officer will disable user access when there is a breach that endangers the security of electronic PHI.
10. If a workforce member changes role, the workforce member's new supervisor or manager is responsible for evaluating the member's current access and for requesting new access to Electronic PHI commensurate with the workforce member's new role and responsibilities.
11. The Security Officer may make exceptions to these access procedures for the following:
 - a. To comply with a legitimate request from public health or law enforcement officials;
 - b. To ensure continued operations of the organization in the presence of temporary mechanical or technical interruption;
 - c. To ensure continued operations of the organization when temporarily or permanently replacing a workforce member who has access to Electronic PHI; or
 - d. To audit the effectiveness of these Policies.
12. The Security Officer has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if the facility declares an emergency or is responding to a natural disaster that makes the management of plan information security secondary to immediate personnel safety activities or management determines that granting immediate access is in the best interest of plan participants.
13. If the Security Officer grants emergency access, he shall review the impact of emergency access and document the event within 24 hours of it being granted.
14. After the emergency event is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.
15. It may be necessary for the Security Officer to grant emergency access to a user's account without the user's knowledge or permission. This access may be granted if:

- a. The workforce member terminates or resigns and management requires access to the person's data;
- b. The workforce member is out for a prolonged period; or
- c. The workforce member has not been in attendance and therefore is assumed to have resigned.

E. Authentication & Password Management

POLICY:

The Plan Sponsor shall ensure that all information systems shall uniquely identify and authenticate workforce members. Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of Plan Sponsor's entire network. As such, all worksite employees are responsible for taking the appropriate steps to select and secure their passwords.

PROCEDURES:

1. Passwords to any systems containing PHI must be changed every 30 days or at such other frequency as provided in the Plan Sponsor's general IT policy.
2. Passwords should be constructed consistent with the Plan Sponsor's general IT policy and procedures.
 - A. Passwords should contain at least 6 characters.
 - B. It is recommended that passwords contain characters from the four primary categories, including: uppercase letters, lowercase letters, numbers, and characters.
 - C. Passwords should never contain the workforce member's personal information (e.g., name, birthday, company name, etc.).
3. Passwords must not be inserted into email messages or other forms of electronic communication unless protected.
4. Passwords should not be shared with others. In cases where password sharing is unavoidable, restricted accounts should be established to protect information resources.
5. If passwords need to be written down or stored on-line, they must be stored in a secure place separate from the application or system that is being protected by the password.
6. The "Remember Password" feature should not be used by any workforce member unless the system or application has the means to encrypt the "remembered password."
7. If an account or password is suspected to have been compromised, the workforce member shall report the incident to the Security Officer and change all passwords.

F. Log-In Monitoring

POLICY:

To ensure that computers and workstations containing Electronic PHI are appropriately secured, the Plan Sponsor will configure all critical components that process, store or transmit Electronic PHI to record log-in attempts and lock in accordance with standard security policy and procedures.

PROCEDURES:

1. Multiple failed login attempts on each system containing Electronic PHI will be logged and documented.
2. The Security Officer or his designee will review such log-in activity reports and logs on a periodic basis.
3. All failed log-in attempts of a suspicious nature, such as continuous attempts, must be reported immediately to the Security Officer.

G. Facility Access Controls

POLICY:

The Plan Sponsor shall reasonably safeguard Electronic PHI from any intentional or unintentional use or disclosure and shall protect its facilities where Electronic PHI is located. The Plan Sponsor shall safeguard the equipment therein from unauthorized physical access, tampering, and theft. The Security Officer shall periodically audit Plan Sponsor facilities to ensure Electronic PHI safeguards are continuously being maintained.

PROCEDURES:

1. Workforce members should not share access cards, hard key access, or alarm or keypad codes.
2. In facilities where Electronic PHI is available, all visitors shall be escorted and monitored. Each facility shall implement procedures that govern visitor access controls that vary depending on facilities structure, type of visitors, and where Electronic PHI is accessible.
3. If facilities use metal/hard keys, the appropriate key locks shall be changed when keys are lost or a workforce member leaves without returning a key.
4. Every network closet shall be locked whenever the room is unoccupied or not in use.
5. Every server room shall be locked whenever the room is unoccupied or not in use.
6. Repairs or modifications to any physical security (e.g., replacement of locks) for each facility where Electronic PHI can be accessed shall be logged and tracked by the Plan Sponsor.

H. Workstation Use & Security

POLICY:

The Plan Sponsor shall establish procedures for securing workstations that access Electronic PHI. Since Electronic PHI may be portable, this Policy requires workforce members to protect Electronic PHI in all locations.

PROCEDURES:

1. All workstations required their own unique identification and passwords.
2. Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access on computer screens by logging out of all files or programs that contain Electronic PHI when leaving their workstation.
3. Workforce members who work from home or other non-office sites shall take the necessary steps to protect Electronic PHI from other persons who may have access to their home or other non-office sites, including password protection on personal computers, and security for all other forms of Electronic PHI such as locking smart phones, and laptops.
4. Workforce members shall always have the user session-lock implemented when any computer or device they use to access Electronic PHI is left idle.
5. Workforce members shall enable the automatic log off and/or screen locking so that computers with Electronic PHI are protected during periods of inactivity. The automatic log off and/or screen locking should block further access until the workforce member reestablishes the connection using the identification and authentication process.
6. The Plan Sponsor will take corrective action against any person who knowingly violates the security of workstation use.

I. Device & Media Controls

POLICY:

The Plan Sponsor shall ensure that Electronic PHI stored or transported on storage devices and removable media is appropriately controlled and managed. This Policy covers accountability, media re-use, disposal, and data backup and storage.

PROCEDURES:

1. Workforce members shall protect all the hardware and electronic media that contain Electronic PHI. This includes, but is not limited to, personal computer, smart phones, laptops, storage systems, backup tapes, photo copiers, CD Rom disks, USB drives, or any removable media.
2. Workforce members will only be granted access to the Plan Sponsor's network from outside devices if the devices are approved by the Plan Sponsor. All other network access options are strictly prohibited.
3. Workforce members shall protect Electronic PHI when working from all other locations, including home.
4. In order to limit the amount of portable Electronic PHI, workforce members shall not save Electronic PHI on USB drives or other portable items or devices. The Electronic PHI must be stored either on the network or an electronic media that can be retrieved in an emergency.
5. If Electronic PHI is lost, workforce members are responsible to promptly contact the Security Officer within one business day upon awareness that Electronic PHI is lost.
6. All Electronic PHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the Electronic PHI or when the equipment is transferred to a new worker with different Electronic PHI access needs. Hard drives shall be wiped clean before transfer. In addition, the hard drive shall be tested to ensure the information cannot be retrieved.
7. All other media shall have all Electronic PHI removed and tested to ensure the Electronic PHI cannot be retrieved before it is disposed of. If the media is not technology capable of being cleaned, the media shall be overwritten or destroyed.
8. When the technology is capable, an exact copy of the Electronic PHI shall be created and the Electronic PHI removed from the server hard drive before sending the device out for repair. If the Electronic PHI is stored on the network, this step is not necessary.
9. Before moving server equipment that contains Electronic PHI, a retrievable copy needs to be created.

J. Transmission Security

POLICY:

Electronic PHI that is transmitted over an electronic communications network shall be protected against unauthorized access to, or modification of, Electronic PHI. When Electronic PHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.

PROCEDURES:

1. When the Security Officer feels it is necessary to protect the security of Electronic PHI, Electronic PHI will be encrypted while at rest.
2. When possible, Electronic PHI being sent outside of the Plan Sponsor's domain will be sent encrypted.
3. When communicating internally, no encryption is necessary.
4. Electronic PHI should not be sent over a wireless network that is not utilizing an authentication and encryption mechanism, unless the Electronic PHI is encrypted before transmission.

K. Protection From Malicious Software

POLICY:

The Plan Sponsor will take all reasonable measures to ensure that computers that may be used to access, receive, transmit or otherwise use Electronic PHI will be protected from viruses, worms or other malicious codes.

PROCEDURES:

1. All computers owned, leased or operated by the Plan Sponsor will have anti virus software and/or endpoint detection and response (EDR) installed and maintained.
2. Workforce members are unable to disable the automatic virus scanning or EDR feature.
3. All downloadable files shall be checked for malware prior to use.
4. The Security Officer or his/her designee shall provide security reminders to the workforce to inform them of any new malware or other type of malicious code that may be a threat to Electronic PHI.
5. Workforce members are instructed to immediately contact the IT department if malware or other malicious code is suspected or detected.
6. In the event that malware or other malicious code has infected or been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately cleaned.

L. System Audits, Audit Controls & Activity Review

POLICY:

The Security Officer or his/her designee follow and apply standard security policy and procedures to regularly review records of information system activity to ensure that implemented security controls are effective and the Electronic PHI has not been potentially compromised.

PROCEDURES:

1. The Security Officer is responsible for auditing information system access; this responsibility may be satisfied through contracting with an outside vendor.
2. The Security Officer shall determine the systems or activities that will be tracked by:
 - a. Focusing efforts on areas of greatest risk and vulnerability as identified in the risk assessment.
 - b. Assessing the appropriate scope of system audits based on the amount of Electronic PHI that the Plan maintains.
 - c. Assessing available organizational resources.
3. The information reviewed will include, but not be limited to, audit logs, access reports, and security incident tracking reports.
4. Audits may be conducted to ensure integrity, confidentiality, and availability of information and resources.
5. Apply standard security policy and procedures when conducting audits to investigate possible security incidents to ensure conformance with the security policies.
6. Apply standard security policy and procedures when conducting audits to ensure virus protection is being maintained at correct levels.

M. Response and Reporting

POLICY:

The Plan Sponsor will identify and respond to suspected or known security incidents. The Plan Sponsor will mitigate the harmful effects of known or suspected security incidents to the extent possible and document the security incidents and their outcomes. It is imperative that this Policy be followed when responding to security incidents.

PROCEDURES:

1. All security incidents, threats, or violations that affect or may affect the confidentiality, integrity or availability of Electronic PHI shall be reported and responded to promptly.
2. Incidents that shall be reported include, but are not limited to:
 - a. Virus, worm, or other malicious code attacks;
 - b. Network or system intrusions;
 - c. Persistent intrusion attempts from a particular entity;
 - d. Unauthorized access to Electronic PHI, an Electronic PHI based system, or an Electronic PHI based network, Electronic PHI data loss due to disaster, failure, error, theft;
 - e. Loss of any electronic media that contains Electronic PHI;
 - f. Loss of the integrity of Electronic PHI; and
 - g. Unauthorized person found in a covered component's facility where PHI is located.
3. The Security Officer shall be notified immediately of any suspected or real security incident. If it is unclear as to whether a situation is a security incident, the Security Officer shall be contacted to evaluate the situation.
4. Any incidents that potentially violate the Plan's security practices or procedures should be reported directly to the Security Officer.
5. The Security Officer shall resolve the incident when possible.
6. The Security Officer shall evaluate the report to determine if an investigation of the incident is necessary.
7. The Security Officer shall determine if the incident is a breach and if it is a Breach the procedures in the Breach policy should be followed.

8. The Security Officer shall train personnel in their incident response roles and responsibilities and provide refresher training as needed.
9. The Security Officer shall test the incident response capability periodically using tests and exercises to determine the effectiveness.

N. Contingency Plan

POLICY:

The Plan Sponsor needs to have procedures in place to continue any necessary Plan activities when normal resources are not available. These procedures will be used in the event of an emergency, disaster or other occurrence (e.g., fire, vandalism, system failure or natural disaster) when any system that contains Electronic PHI is affected, including: applications and data criticality analysis, data backup, disaster recovery plan, and emergency mode operation plan. Since the Plan Sponsor maintains very little Electronic PHI on its systems and what it does maintain is information also maintained by outside service providers, this procedures should rarely, if ever, need to be implemented.

PROCEDURES:

Applications and Data Criticality Analysis

1. The Security Officer shall assess the relative criticality of specific applications and data for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
2. The Security Officer shall identify critical business functions, define impact scenarios, and determine resources need to recover from each impact, if any.
3. The assessment of data and application criticality shall be conducted periodically to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup

4. All Electronic PHI shall be stored on network servers in order for it to be automatically backed up by the system consistent with the Plan Sponsor's information technology procedures.
5. Electronic PHI shall not be saved on the local drives of personal computers.
6. Electronic PHI shall not be stored on portable media and shall be saved to the network to ensure backup of Electronic PHI data.
7. The system shall conduct backups of user-level and system-level information and store the backup information in a secure location.
8. If an off-site storage facility or backup service is used, a written contract shall be used to ensure that the contractor shall safeguard the Electronic PHI in an appropriate manner.

Disaster Recovery Plan

9. Due to the Plan Sponsor and Plan having very limited access to Electronic PHI, the Security Officer determined that there is no Electronic PHI that a workforce member would need to immediately recover in an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster. Backup media is stored off-site and could be recovered within reasonable timeframes.
10. The Security Officer will reevaluate whether a disaster recovery plan is necessary periodically.

Emergency Mode Operation Plan

11. Due to the Plan Sponsor and Plan having very limited access to Electronic PHI, the Security Officer determined that an emergency mode plan is not necessary because all Electronic PHI that may be needed in an emergency is maintained with Business Associates of the Plan.
12. The Security Officer will reevaluate whether an emergency mode operation plan is necessary periodically.

O. Disposal of ePHI

POLICY:

The Plan Sponsor shall dispose of ePHI pursuant to its adopted retention policy.

PROCEDURES:

Retention Policies

Each Appointing Authority has adopted a retention schedule in addition to the County-wide general retention schedule. ePHI shall be addressed in those policies and shall be retained and/or destroyed pursuant to those policies.

Resolution

Number 25-0241

Adopted Date February 25, 2025

CANCELLING THE REGULARLY SCHEDULED COMMISSIONERS' MEETING OF
THURSDAY, FEBRUARY 27, 2025

BE IT RESOLVED, to cancel the regularly scheduled Commissioners' Meeting of Thursday,
February 27, 2025.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon
call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

/kp

cc: Auditor ✓
Commissioners' file
Press

Resolution

Number 25-0242

Adopted Date February 25, 2025

ADVERTISING FOR THE 2025 PRECAST REINFORCED CONCRETE BOX CULVERTS PROJECT

BE IT RESOLVED, to advertise for the 2025 Precast Reinforced Concrete Box Culverts Project for the County Engineer; and

BE IT FURTHER RESOLVED, to advertise said bid for one (1) week in a newspaper of general circulation and for two consecutive weeks on the County website, beginning the week of March 2, 2025; bid opening to be March 17, 2025 @ 10:30 a.m.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

KP

cc: Engineer (file)
Bid file

Resolution

Number 25-0243

Adopted Date February 25, 2025

APPROVING NOTICE OF INTENT TO AWARD BID TO NEYRA PAVING FOR THE FY24 SOUTH LEBANON KING AVENUE STREET IMPROVEMENTS CDBG PROJECT

WHEREAS, bids were closed at 10:30 a.m., on February 12, 2025, and the bids received were opened and read aloud for the FY24 South Lebanon – King Avenue Street Improvements CDBG Project, and the results are on file in the Commissioners' Office; and

WHEREAS, upon review of such bids by Susanne Mason, Director, Neyra Paving has been determined to be the lowest and best bidder.

NOW THEREFORE BE IT RESOLVED, upon recommendation of the Warren County Office of Grants Administration, that it is the intent of this Board to award the contract to, Neyra Paving, 10750 Evendale Drive, Cincinnati, Ohio 45241 for a total bid price of \$83,622.10; and

BE IT FURTHER RESOLVED, that the President of the Board is hereby authorized to execute a "Notice of Intent to Award."

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: OGA (file)
OMB Bid file

Resolution

Number 25-0244

Adopted Date February 25, 2025

AUTHORIZING THE PRESIDENT OF THE BOARD TO SIGN MEMORANDUM OF UNDERSTANDING WITH TEAM RUBICON ON BEHALF OF THE WARREN COUNTY DEPARTMENT OF EMERGENCY SERVICES

WHEREAS, Warren County Emergency Services desires to enter into an agreement with Team Rubicon for the purpose of setting the terms by which Warren County Ohio Emergency Management and Team Rubicon will cooperate regarding disaster response and community disaster recovery, including but not limited to damage assessments/site surveys, debris management, hazard mitigation, repair work, and demolition; and

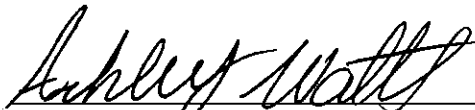
NOW THEREFORE BE IT RESOLVED, to authorize the President of the Board to sign the Memorandum of Understanding with Team Rubicon on behalf of Warren County Emergency Services; copy of said Memorandum of Understanding attached hereto and made a part hereof.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: c/a—Team Rubicon
Emergency Services (file)

MEMORANDUM OF UNDERSTANDING

Between

Warren Co. Ohio Emergency Management

an agent of Warren County, Ohio

And

Team Rubicon

Parties

The Parties to this Memorandum of Understanding (MOU) are the Warren Co. Ohio Emergency Management as an agent of Warren County, Ohio and Team Rubicon (TR).

PURPOSE

The purpose of this agreement is to set forth the terms by which Warren Co. Ohio Emergency Management and TEAM RUBICON will cooperate regarding disaster response and community disaster recovery including but not limited to damage assessments/site surveys, debris management, hazard mitigation, repair work, and demolition.

RESPONSIBILITIES

Warren Co. Ohio Emergency Management agrees to, as appropriate:

1. Designate a liaison to coordinate assistance with TEAM RUBICON and area officials affected by disasters.
2. Collaborate with TEAM RUBICON on joint training, exercises, and/or workshops.
3. Assist TEAM RUBICON by identifying best practices, resources, and partnership opportunities as requested.
4. Share with TEAM RUBICON messages and information regarding volunteering at disaster sites.
5. Establish appropriate lines of communications between local county officials and a TEAM RUBICON liaison.

TEAM RUBICON agrees to, as appropriate:

1. Share with Warren Co. Ohio Emergency Management policy and guidance manuals, brochures, videos, and other information and training resources regarding their methods for support during response and recovery.
2. Disseminate Warren Co. Ohio Emergency Management information through its staff and volunteers.
3. Encourage members to comply with civil rights laws that ensure equal opportunity for people with disabilities when working with state government.
4. Provide input and feedback to the emergency management plan, relevant annexes or other documents, as appropriate.
5. Engage in joint projects with Warren Co. Ohio Emergency Management, as appropriate, promoting the common mission of efficient and effective public service in emergency management.
6. Assist Warren Co. Ohio Emergency Management when a state of disaster emergency has been proclaimed by the State of Ohio by designating an agency liaison to work with Warren Co. Ohio Emergency Management recovery staff.
7. Work closely with Warren Co. Ohio Emergency Management liaisons in convening meetings and conference calls in response to disasters, and to share information about

field disaster response, recovery and mitigation activities with Warren Co. Ohio Emergency Management.

8. All services performed by TR under this Agreement must be initiated by a request for assistance from Warren Co. Ohio Emergency Management. Such requests for assistance from TR do not have to be directly related to an ongoing event. Requests for Assistance (RFA) will be made via telephone or email to the TR Point of Contact.
9. TR may accept or decline requests, depending on staff and equipment availability. TR will confirm their decision via email to Warren Co. Ohio Emergency Management.

OTHER PROVISIONS

- A. This MOU imposes no enforceable obligations upon the Parties. Warren Co. Ohio Emergency Management and TEAM RUBICON may utilize this MOU as the framework for an agreement(s).
- B. Nothing in the MOU is intended to restrict the authority of either Party to act independently and as provided by law, statute, or regulation.
- C. Nothing in this MOU shall be interpreted as affording Warren Co. Ohio Emergency Management or TEAM RUBICON any role in the content or programming decisions of either the agency or the organization, respectively.
- D. In order to facilitate and accomplish the goals and objectives set forth in this MOU, TEAM RUBICON and Warren Co. Ohio Emergency Management will meet as necessary and appropriate to discuss issues of mutual interest and assess progress on accomplishing the desired objectives.
- E. This MOU is not a fiscal or funds obligation document and does not guarantee funding. Each Party shall be responsible for its own costs related to activities under this MOU and neither Party shall be required to reimburse the other for any expenses related to activities under this MOU.
- F. This MOU is not entered into with the intent that it shall benefit any other person and no other such person shall be entitled to be treated as a third-party beneficiary of this MOU.
- G. This MOU neither creates a partnership nor a joint venture, and neither Party has the authority to bind the other.
- H. The Parties acknowledge that Warren County is governed by the Ohio Public Records Laws. Notwithstanding any statement in this MOU to the contrary, Warren County's handling of any confidentiality obligations are subject to the limitations of this paragraph. Records (as defined by Ohio Revised Code §§ 149.011 and 149.43) related to this MOU may be subject to disclosure under the Ohio Public Records Laws. Warren County shall have no duty to defend the rights of TEAM RUBICON or any of its agents or affiliates in any records requested to be disclosed. Upon receipt of a public records request, Warren County will notify TEAM RUBICON of its intent to release records to the requestor. TEAM RUBICON shall have a maximum of five (5) business days beginning with the date it receives notification to respond to Warren County by either accommodating the requestor or pursuing legal remedies to stop the Warren County's release of requested information. Said notification shall relieve the Warren County of any further obligation under any claim of TEAM RUBICON or any of its agents or affiliates in any jurisdiction in connection with the disclosure of such records. TEAM RUBICON and its agents and affiliates shall have the right to pursue legal and/or equitable remedies to stop or limit disclosure at their sole expense.
- I. Each Party to this MOU agrees to be liable for the negligent acts or negligent omissions, intentional or wrongful acts or omissions, by or through itself, its employees and agents. Each Party further agrees to defend itself and pay any judgments and costs arising out of such negligent, intentional, or wrongful acts or omissions, and nothing in this MOU shall impute or transfer any such liability from one Party to the other.
- J. **This MOU is subject to, will be governed by, and construed in accordance with the**

substantive laws in force of the County of Warren, State of Ohio which shall have exclusive jurisdiction over any disputes except in matters of conflict of laws.

EFFECTIVE DATE

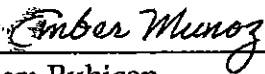
The terms of this memorandum will become effective on the date of the last signature by the Parties as indicated on the signature page of this memorandum.

MODIFICATION

This MOU may be modified upon the mutual written consent of the Parties.


TERMINATION

The term of this memorandum, as modified with the consent of both parties, will remain in effect for one year from the date of the last signature. The memorandum may be extended by mutual written agreement of the parties. In addition, either party may terminate this agreement upon sixty (60) days written notice to the other party.

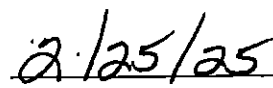


Team Rubicon

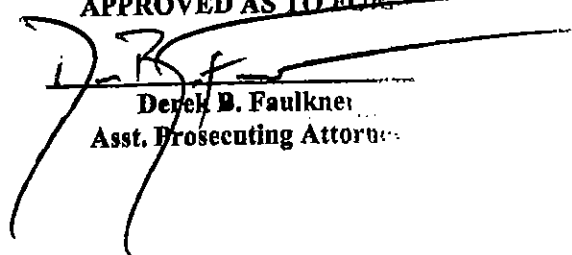
February 3, 2025
Date



Warren Co. Ohio Emergency Management



Date

APPROVED AS TO FORM


Derek B. Faulkner
Asst. Prosecuting Attorney

Resolution

Number 25-0245

Adopted Date February 25, 2025

AUTHORIZING THE PRESIDENT OF THE BOARD TO SIGN A LOCAL SUPPORT AGENCY MEMORANDUM OF UNDERSTANDING WITH WARREN CORRECTIONAL INSTITUTION ON BEHALF OF WARREN COUNTY EMERGENCY SERVICES

BE IT RESOLVED, to authorize the President of the Board to sign the Local Support Agency Memorandum of Understanding with Warren Correctional Institution on behalf of Warren County Emergency Services; copy of said Memorandum of Understanding attached hereto and made a part hereof.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: C/A—Warren Correctional Institution
Emergency Services (file)



**Local Support Agency Memorandum of Understanding
With
EMA & Warren Correctional Institution (WCI)
January 23, 2025**

The Ohio Department of Rehabilitation and Correction Protects Ohio citizens by ensuring effective supervision of adult offenders in environments that are safe, humane and appropriately secure. However, there may be a Critical Incident which disrupts the routine operations or services of a correctional facility creating a state of disorder, a threat to security or an inability to maintain orderly control of inmates. During the course of our response and recovery from the Critical Incident, it may be necessary to utilize resources beyond what ODRC is able to directly provide.

I. Statement of Purpose

The Purpose of this Memorandum of Understanding is to identify resources that can be made available by the Warren County Department of Emergency Services to the Warren Correctional Institution to assist in response and recovery of a Critical Incident occurring at the prison. This memorandum is developed to provide a planning guide for the prison to know the agency's capabilities to respond to a Critical Incident. However, this memorandum does not guarantee that any or all services, personnel, and/or equipment will be available at all times.

NOTE: The Department of Emergency Services is the Emergency Management Authority for Warren County, Ohio.

II. Request for Assistance

In the event of a Critical Incident in the prison, the agency will be contacted by a prison employee in the ICS Logistics Section. Requests for local Emergency Management resource assistance will be made by the following process.

- A. Call the Warren County Communication Center at (513) 695-2525 and request the Supervisor or Operator in Charge.
- B. Provide:
 - a. The nature of the Critical Incident
 - b. The assistance needed (type, kind, quantity, and time to report).
 - c. The location to which they are to respond.

Warren Correctional Institution
5787 State Route 63
Lebanon, OH 45036

513 | 932 3388

drc.wci@odrc.state.oh.us



- d. The person to whom they are to report to upon arrival.
- e. A contact name and number.

C. Request the Communication Center to page the Emergency Management Staff.

In the event of a Critical Incident in Warren County, Warren Correctional Institution will be contacted by a county employee. Requests for local resource assistance will be made by the following process.

- A. Call Warren Correctional Institution at (513) 932-3388 and request for a Shift Commander in charge.
- B. Provide:
 - a. The nature of the Critical Incident.
 - b. The assistance needed (type, kind, quantity and time to report).
 - c. The location to which they are to respond.
 - d. The person to whom they are to report to upon arrival.
 - e. A contact name and number.

III. Scope of Assistance

The Local Support Agency resources are understood to be available to the prison on a twenty-four (24) hour a day, seven (7) day a week basis, unless otherwise specified in this Memorandum of Understanding.

A. The Personnel Resource response by the agency to the prison is as follows:

- 1. Director of Emergency Services
- 2. Emergency Management Operations Manager
- 3. LEPC Coordinator
- 4. Communications and Telecommunications Personnel as deemed necessary by the Director and Incident Commander

B. The Equipment Resource response by the agency to the prison is as follows:

- 1. 800MHz Radios which include the Marcs and Warren County Systems
- 2. Cellular Telephones

Warren Correctional Institution
5787 State Route 63
Lebanon, OH 45036

513 | 932 3388

drc.wci@odrc.state.oh.us



C. The Support Services capabilities of the agency to the prison is as follows:

1. Acquisition Resources
2. On Scene Resource Coordination
3. Communication Coordination with Responders
4. Search & Rescue Coordination
5. Activation of County Emergency Operation Center
6. Direct Avenue of Control with Ohio Emergency Management Agency's E.O.C. via Radio, Fax, and/or Telephone for State Coordination of Resources

D. The agency utilizes the following radio frequencies:

Warren County operates on the Ohio MARCS system.

The Local Support Agency resources are understood to be available to Warren County on a twenty-four (24) hour a day, seven (7) day a week basis, unless otherwise specified in this Memorandum of Understanding.

A. The Support Services capabilities of Warren Correctional to Warren County is as follows:

1. In the need of an emergency evacuation of the Warren County jail, Warren Correctional Institution can provide four (4) - twelve (12) passenger transportation vans, and one (1) forty-two (42) passenger HUB bus. The HUB bus will be provided by WCI only if it is not being utilized by the institution at the time of the emergency evacuation.

IV. Prison/ Agency Responsibilities

The Incident Commander will designate an individual to coordinate the agency's assistance and needs in response to the Critical Incident. This individual will coordinate all security and any other needs of the agency, which may include, but not be limited to: Specific security issues, access to facilities, and protection of equipment and personnel. The prison will work with the agency to identify and arrange for the availability of utility connections at each prison site to facilitate the utilization of the agency resources. By ODRC policy, the prison Incident Commander has been delegated authority to manage a Critical Incident. However, where there is active involvement of Local Support Agencies, a Unified Command structure may be established, and command authority would then be shared with assisting agencies. The Incident Commander and the prison Incident

Warren Correctional Institution
5787 State Route 63
Lebanon, OH 45036

513 | 932 3388

drc.wci@odrc.state.oh.us



Command Organization will work closely with the agency to coordinate their response. To maintain effective information release, the prison's Public Information Officer shall coordinate the Public/Media Information Release. The Local Support Agency shall consult with the prison's Public Information Officer prior to the release of information.

V. Annual Review of the Memorandum of Understanding

The Warren Correctional Institution and the Warren County Department of Emergency Services will conduct an annual review of the details of this Memorandum of Understanding. Once updated, the prison will re-issue this document.

VI. Limitation of Liability

The Warren County Board of County Commissioners and its Department, Agencies and Employees shall not be liable to ODCR, its employees, agents, or officers, or to third parties for claims, damages, expenses, costs, fees, attorney fees, injurious actions, causes of actions or suits due to a refusal or failure to respond, in whole or in part, to a request for assistance.

Capt. C. Barrett
Warren Correctional Institution

Date: 1-30-25

Warren County Board of Commissioners

Date: 2/25/25

Warren County Prosecutor's Office

Date: February 18, 2025

Warren Correctional Institution
5787 State Route 63
Lebanon, OH 45036

513 | 932 3388

drc.wcl@odrc.state.oh.us

Resolution

Number 25-0246

Adopted Date February 25, 2025

ENTERING INTO A YOUTH WORKSITE AGREEMENT ON BEHALF OF
OHIO MEANS JOBS WARREN COUNTY

BE IT RESOLVED, to enter into Youth Worksite Agreement with the following company, as attached hereto and made part hereof:

Kirby's Auto & Truck Repair
875 Coumbus Ave
Lebanon, Ohio 45036

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: c/a – OhioMeansJobs Warren County
OhioMeansJobs (file)

**OhioMeansJobs Warren County
TANF Youth Employment Program
Worksite Agreement**

This agreement is entered into by and between on this 6th day of Feb, 2025, between the Warren County Board of Commissioners on behalf of the OhioMeansJobs Warren County, 300 East Silver St, Lebanon, Ohio 45036, hereinafter referred to as OMJWC, Kirby's Auto & Truck Repair, 875 Columbus Avenue, Lebanon, Ohio 45036, hereinafter referred to as Worksite, for the employment of youth as authorized by the TANF Summer Youth Employment Program from date of action by the Board of Commissioners through June 30, 2026.

WITNESSETH:

WHEREAS, OMJWC operates a TANF Work Experience Program which may provide temporary entry level employment experiences to eligible Warren County youth from age 14 through age 24 years; and

WHEREAS, eligible worksites are needed for TANF Work Experience Program participants; and

WHEREAS, the Worksite desires to participate in the TANF Work Experience Program by providing employment opportunities for youth at the above named worksite location.

NOW THEREFORE, in consideration of the promises and mutual covenants herein set forth, it is agreed by and between the parties hereto as follows:

- A. OMJWC in conjunction with Southwest Ohio Council of Governments will provide youth recruitment, intake and job placement; payroll preparation and distribution; youth counseling; worksite visitation/evaluation; and other TANF Work Experience Program services for youth and technical assistance to the Worksite and youth, as required.
- B. OMJWC is mandated by law to serve only low income youth with identified barriers, as defined by the TANF Summer Youth Employment Program and Ohio's Comprehensive Case Management and Employment Program(CCMEP). The Worksite, in operating programs funded under the TANF Work Experience Program, assures that it will administer its program in full compliance with safeguards against fraud and abuse as set forth in the program regulations; that no portion of its TANF Work Experience Program will in any way discriminate against, deny services to or exclude from participation any person on the grounds of race, color, national origin, religion, age, sex, handicap or political affiliation or belief; and that it will target employment and training services to those most in need of them and best able to benefit from them.
- C. Timesheets, signed by the participant and the worksite supervisor, will be on file in the OMJWC office. The following information will be available in the TANF

Work Experience Program records and/or the participant's file: name and age of participant, application, employment questionnaire, job location, job title and job description. Worksite information will be included in Attachment A of the Worksite Agreement. Additional participants may be added throughout the duration of the Worksite Agreement.

- D. Youth may be required to attend TANF Summer Youth required training sessions and seminars. These will be scheduled in advance in collaboration with the Worksite Supervisor and the TANF Work Experience Program Supervisor and Coordinator. In the event that a session takes place during the youth's regularly scheduled work time, the total time spent in paid training cannot exceed the number of hours permitted for that particular day as specified in this agreement.
- E. OMJWC or its authorized representative, the Secretary of Labor or his/her authorized representative(s) and the Governor of the State of Ohio or his/her authorized representative(s) may at all times have the right to access, and inspect when necessary and without prior notice, the place of work under this agreement and any records pertinent to this agreement, to assure the progress and quality of training or to determine compliance with the agreement's terms.
- F. The Worksite agrees that the services of the TANF Work Experience Program participants will not displace regular employees, but will be used to augment the regular workforce or for special programs designed for youth. Further, any Worksite that has laid-off an employee within a requested job classification will not have its request filled until twelve months from the date that the lay-off occurred.
- G. The Worksite agrees that youth will not be involved in programs or activities which are in violation of Federal or State regulations, as amended, governing religious/sectarian or political activities.
- H. The Worksite shall save and hold harmless OMJWC, OhioMeansJobs of Warren County, the Board of Warren County Commissioners and their employees from liability of any nature arising from the participation in TANF Summer Youth funded programs, including, but not limited to: cost and expenses for or on account of any suits or damages of any character whatsoever resulting from injuries or damages sustained by persons or property resulting in whole or in part from negligent performance or omission of an employee, agent or representative of the Worksite, as well as the youth and other individuals working for the Worksite agency pursuant to this agreement.
- I. The Worksite agrees to provide, at their expense, adequate and qualified adult supervision. The Worksite must be responsible for assuring the Worksite Supervisors comply with the requests of the TANF Work Experience Program Coordinator regarding issues related to TANF Work Experience Program participants and in particular, maintain accurate youth timesheets. The Worksite Supervisor will be held responsible for keeping accurate records of hours worked by each youth.

The Worksite agrees to maintain open communication with monitoring staff assigned to the site and to reply to requests for information in a timely manner.

Wages requested must be for hours worked (or spent in OMJWC approved training/counseling sessions scheduled during regular work hours only). Time sheets must be signed by each youth and his/her supervisor before payroll checks can be issued. Records pertinent to this agreement shall be retained by the worksite for the duration of the program and thereafter delivered to OMJWC within seven days to be properly stored.

- J. The Worksite assures that no person under its employment who presently exercises any functions or responsibilities in connection with OMJWC or TANF Summer Youth funded projects or programs, has or had any financial interest, direct or indirect; in this agreement, nor will the Worksite hire any person having such financial interest.
- K. The Worksite assures that it will fully comply with the requirements of the OMJWC, all Federal regulations.
- L. The Worksite agrees to abide by all Federal, State and local labor laws; State of Ohio and Federal Child Labor Law restrictions (Attachment B); Civil Rights Provisions which include, but are not limited to, Title VI and VII of the 1964 Civil Rights Act; Ohio Revised Code 4112; Age Discrimination Enforcement Act; Rehabilitation Act of 1973; as well as any and all amendments thereto.
- M. The Worksite agrees and understands that participation in TANF Work Experience Programs requires no compensation of any kind to either party, and that there will be no compensation of any kind made to the Worksite.
- N. The Worksite shall comply with all Federal and State Occupational Safety and Health Regulations (OSHA) dealing with safety of workers on the worksite. The Worksite shall save and hold harmless OMJWC, OhioMeansJobs of Warren County, The Board of Warren County Commissioners, the Area 12 Council of Governments, Area 12 Workforce Investment Board and their employees, from any and all liability that may arise as a result of an OSHA violation.
- O. Any changes in supervision, Worksite location, work duties or schedule for youth assigned to the Worksite, or any other changes in this Agreement, will be made only with prior written notification to and written approval from the OMJWC TANF Work Experience Program Coordinator. Failure to follow this procedure may result in immediate termination of the Worksite Agreement at the sole discretion of OMJWC.
- P. The Worksite and the OMJWC understand and agree that signing of this agreement does not guarantee the placement of youth at the Worksite(s). OMJWC will notify the Worksite if there will be a reduced number or no

placement of youth due to the unavailability of youth within fifteen (15) days after the beginning of the program.

Q. This agreement may be terminated without cause ten days following the receipt of written notice of termination given by either party. This agreement may be immediately terminated without legal or financial liability of OMJWC for the causes listed below:

1. If supervision provided is deemed inadequate;
2. If there is insufficient work for the youth;
3. If there is a lack of funds or if funding becomes unavailable to the OMJWC;
4. If the Worksite refuses to accept any additional conditions that may be imposed upon the Worksite by the Department of Labor, the State of Ohio Department of Job and Family Services or the OMJWC or if the Worksite, in the sole opinion of the OMJWC, fails to comply with any provisions of this agreement or any provision of the TANF Work Experience Program or any memorandum, policy, bulletin, etc. of the Ohio Department of Job and Family Services or the OMJWC.

R. **INSURANCE**

Vendor (worksite) shall provide liability insurance coverage as follows:

Vendor (worksite) shall carry Comprehensive General Liability coverage or Professional Liability coverage with limits of \$1,000,000 Per Occurrence, \$2,000,000 / Aggregate, with no interruption of coverage during the entire term of this Agreement. *[if applicable]* Vendor (worksite) shall also carry automobile liability coverage with limits of \$1,000,000 Per Occurrence / Aggregate.

Vendor(worksite)further agrees that if any Comprehensive General Liability or Professional Liability coverage is on a "claims made" basis, the policy provide that in the event this Agreement is terminated, Vendor (worksite) shall continue such policy in effect for the period of any statute or statutes of limitation applicable to claims thereby insured, notwithstanding the termination of the Agreement.

By endorsement to the Comprehensive General Liability or Professional Liability coverage, Warren County shall be named as an additional insured with the same primary coverage as the principal insured – no policy of Comprehensive General Liability or Professional Liability coverage that provides only excess coverage for an additional insured is permitted.

Vendor (worksite) shall provide Warren County with a certificate of insurance evidencing such coverage and conditions set forth herein, and shall provide thirty (30) days notice of cancellation or non-renewal to Warren County. Such certificates shall provide that the insurer notify Vendee in writing should any of the above described policies be canceled before the expiration date thereof, to be mailed by the insurer to the Vendee not less than 30 days prior to said cancellation date.

Vendor (worksite) shall also deliver to Lessor, at least 15 days prior to the expiration date of each policy or policies (or of any renewal policy or policies), certificates for the renewal policies of the insurance coverage required herein.

S. This agreement may be modified upon mutual consent of both parties.


T. **GROUPS FOR DISCIPLINARY ACTION AND PENALTIES.** Upon enrollment, each youth will be given work rules and the disciplinary policies (Attachment C) which is included in the Youth's Participant Manual. If the Worksite has any additional rules which shall apply to the youth's conduct, these shall be indicated in the space provided below. The Worksite may add rules or reinforce rules, but no rules may be deleted from Attachment C. It is agreed that the rules indicated in Attachment C will be in effect at the Worksite.

Rule:	Group:
Proper foot wear required	Weld shop / Auto shop
Safety Glasses / gloves	" "
Ear protection - provided	" "

U. **CERTIFICATIONS:** The undersigned individuals have read and fully comprehend all statements in this Worksite Agreement and signify by their signatures a voluntary intent to be fully bound by the provisions of this agreement as well as any and all attachments which are explicitly merged and incorporated into the agreement. In addition, the organized labor representative, if applicable, reviewing this agreement expressly stipulated by his/her below affixed signature that he/she has read, understands and voluntarily concurs with the Worksite Agreement. A copy of the completed Worksite Agreement will be returned to the Worksite Administrator after being reviewed and signed by the OMJWC representative. The Worksite is to retain its copy of the Worksite agreement in its files for the duration of the program year.

IN WITNESS WHEREOF, the parties have executed this Agreement on this 25
day of February, 2025.

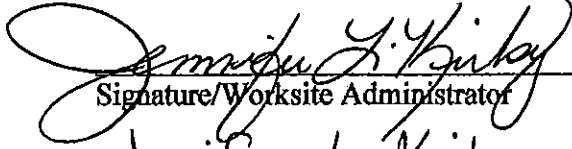
WARREN COUNTY BOARD OF COMMISSIONERS:



David C. Young, President
Tom Grossmann

WORKSITE:

Kirby's Auto + Truck Repair, Inc. / Warren Welding & Fabrication
Worksite Name



Signature/Worksite Administrator
Jennifer L. Kirby

Title of Worksite Administrator

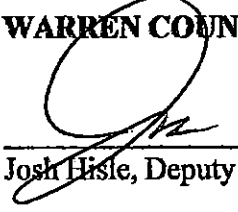
Feb. 6, 2025
Date

If applicable, an Organized Labor Representative should review this agreement and stipulate by his/her signature below that he/she has read, understands, and voluntarily concurs with the execution of the Worksite Agreement.

Signature of Authorized Organized Labor Representative

Date

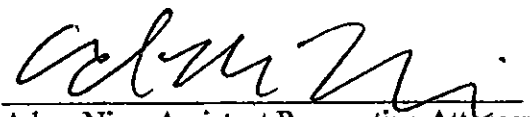
WARREN COUNTY JFS, DIVISION OF HUMAN SERVICES



Josh Hisle, Deputy Director

2-18-25
Date

APPROVED AS TO FORM:



Adam Nice, Assistant Prosecuting Attorney

III. Job Description(s): Each worksite, even if located in the same building (i.e. clerical and custodial) should be listed as a separate worksite.

Worksite #1 Welding & Fabrication - Job Shop

Worksite #2 Auto & Truck Repair/Service Shop

Worksite #3 _____

Worksite #4 _____

Worksite #5 _____

IV. Additional Information:

Is your agency planning to have youth use power-driven machinery and/or perform any "hazardous occupational orders"? (Please refer to Child Labor Laws)

Yes No If yes, please describe the type of power-driven machinery to be used and/or "Hazardous" work tasks.

With instruction - Weed eater or yard equipment.
After training car lift, hand tools, air compressor, etc.
Depending on skill level other equipment may be inc.

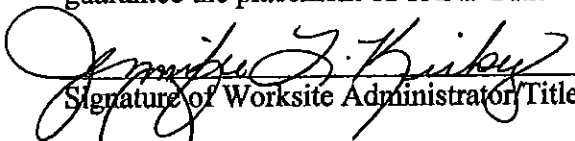
Training and safety instructions must be provided by worksite personnel if skilled or special equipment is required to perform the tasks described in this agreement. Youth work activities are governed by the applicable State and Federal Child Labor Laws.

If weather or other factors do not permit the regularly scheduled work to be done, please describe the contingency plan of work duties for youth employees.


N/A

Additional rules or policies to be followed at the worksite during work time are listed in the Worksite Agreement. These rules will be in addition to the disciplinary rules provided in Attachment C of the Worksite Agreement.

The undersigned individuals signify by their signatures that they have read and fully comprehend all statements in this TANF Work Experience Program request Form and that they understand and agree that this is a request form only and that it does not guarantee the placement of TANF Summer Youth at the worksite (s) requested.


Signature of Worksite Administrator Title

02-06-2025
Date


Josh Hisle, Deputy Director, OMJWC

2.18.25
Date

Attachment B

Minor Labor Laws

In accordance with State of Ohio Child Labor Laws, 14 and 15 years olds MAY NOT:

1. Operate electric or gas lawn mowers
2. Operate string or blade trimmers, weed eaters or weed whips.

In accordance with the State of Ohio Child Labor Laws, minors under the age of 16 MAY NOT be involved in the following tasks:

1. Operating a tractor of over 20 PTO (Power take Off) horsepower or connecting or disconnecting an implement of any of its parts to or from such a tractor.
2. Operate a power post hole digger, post driver, or non-walking type rotary tiller or power mover;
3. Operate or assist in the operation of (including starting, stopping, adjusting, feeding or any activity involving physical contact with the operation of)
4. Work from a ladder or scaffold
5. Drive a bus, truck or automobile when transporting passengers.
6. Handle or apply agricultural chemicals classified under the Federal Fungicide and Rodenticide Act (7 U.S.C. 135 et. Seq.) as Category I toxicity, identified by the "skull and crossbones" on the label or Category II of toxicity, identified by the word "WARNING" on the label.
7. Work in connection with cars, trucks or busses involving the use of pits, racks, lifting apparatus or involving inflation of any tire mounted on a rim equipped with a removable retaining ring.

In accordance with the State of Ohio Child Labor Laws, minors under the age of 18 MAY NOT be involved in the following tasks:

1. Operating or helping to operate the following power driven tools:
 - a. Circular saws
 - b. Band saws
 - c. Guillotine shears.
2. Setting up, adjusting, repairing, oiling or cleaning circular saws, band saws or guillotine shears.
3. Excavating, working in or backfilling (refilling) trenches except:
 - a. Manually excavating or manually backfilling trenches that do not exceed (4) feet in depth at any point.
4. Using fertilizers, fungicides, insecticides, rodenticides or herbicides.

When there is disagreement between State and Federal Child Labor Laws, the most restrictive standard is to be used. Attached is a summary of the comparison of the State and Federal requirements.

Attachment C

GROUPS FOR DISCIPLINARY ACTIONS AND PENALTIES

GROUP I OFFENSES

FIRST OFFENSE- Written reprimand

SECOND OFFENSE- Written reprimand, counseling

THIRD OFFENSE – Three days suspension

FOURTH OFFENSE – Termination

1. Failure to call in about missing work – for any reason.
2. Creating or contributing to unsanitary or unsafe conditions, including risking of personal safety (spitting, hitting, etc.)
3. Failure to use reasonable care of agency property or equipment
4. Bringing a friend to the worksite during work hours
5. Not responding to a reasonable request from a supervisor

GROUP II OFFENSES

FIRST OFFENSE – Written reprimand, counseling

SECOND OFFENSE - Three (3) day suspension **WITHOUT PAY**

THIRD OFFENSE- Termination

1. Unauthorized use of agency property or equipment
2. Willful disregard of department rules
3. Use of abusive or threatening language toward supervisors, co-workers or other persons
4. Malicious mischief, horseplay, wrestling or other undesirable conduct

GROUP III OFFENSES

FIRST OFFENSE – Mandatory counseling sessions (determined by degree of offense)

SECOND OFFENSE – Termination

1. Being in possession of or drinking alcoholic beverages or controlled substances without a bona-fide prescription while on the job
2. Wanton or willful neglect in performance of assigned duties or in the care, use or custody of county property or equipment.
3. Abuse or deliberate destruction in any manner of county property or employees
4. Signing or altering other employees' time cards or unauthorized altering of own time card
5. Stealing or similar conduct including destroying, damaging or concealment of any property of the county or other employees
6. Fighting or attempting injury to any other persons.

Attachment A

**Warren Co. TANF Summer Youth Employment Program
Request Form**

I. Agency Information:

Agency Name: Kirby's Auto + Truck Repair, Inc.
 Address: 875 Columbus Ave. Lebanon Ohio 45036
 Phone: 513-934-3999 E-mail Kirbysautorepair@AOL.com
 Agency Administrator: Glen + Jennifer Kirby
 Contact Person: Jennifer Kirby
 FEIN#: 03-0548232

II. Program Information: Work for the youth will begin at the worksite on or about _____ and continue until on or about _____. Be sure that you have enough work for the number of youth you request. Youth will work a maximum of ___ hours per week, normally ___ hours per day. Any request for change in hours, job duties or supervisor must be made in written or verbal form to the One-Stop in advance of the change.

All youth must be supervised. Please review the job description included in the worksite packet, which briefly outlines responsibilities of a Worksite Supervisor. All supervisors must be adequately oriented before a youth may begin work.

Please provide all of the information requested below for each worksite.

Worksite	Name and Phone # of Supervisor	Number of youth requested	Preferred Age of Youth	Schedule of Hours	Interview Requested?
				From: To:	Yes No
				From: To:	Yes No
				From: To:	Yes No
				From: To:	Yes No
				From: To:	Yes No

Resolution

Number 25-0247

Adopted Date February 25, 2025

ENTERING INTO AN AGREEMENT WITH READY TO RENT, LLC ON BEHALF OF
OHIOMEANSJOBS WARREN COUNTY

BE IT RESOLVED, to enter into an agreement with Ready to Rent, LLC for a one-time
licensing fee for unlimited use of curriculum materials on behalf of OhioMeansJobs Warren
County. Copy of agreement is attached hereto and made a part hereof:

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon
call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: c/a—Ready to Rent, LLC
OhioMeansJobs (file)

Ready to Rent® Licensing Agreement

The purpose of this AGREEMENT is to set forth the LICENSING terms and conditions that will govern the use of the Ready to Rent® curriculum and training program.

This AGREEMENT is between Ready To Rent LLC and

Ohio Means Jobs Warren County (AKA Licensee)
(Please Print Agency Name)

Licensing & Fee

The Licensee named above will pay a one-time \$700 fee and have unlimited use of curriculum materials with agency clients. If Licensee discontinues use of the curriculum, Licensee must notify Ready To Rent LLC in writing within 90 days.

Licensing includes:

- The following materials associated with the Ready to Rent Curriculum (provided via the Ready To Rent cloud drive to Instructors):
 - ✓ Standard Ready to Rent Action Kit (participant workbook)
 - ✓ Adapted Ready to Rent Action Kit (participant workbook)
 - ✓ Spanish language Ready to Rent Action Kit (participant workbook, on flash drive only)
 - ✓ Outline of Ready to Rent Orientation in PowerPoint
 - ✓ Essential marketing materials, including program fliers, sample presentation to landlords, and other related materials.
 - ✓ Sample program forms, including forms used in Ready to Rent trainings, forms used to promote and administer the Ready to Rent program.
- Licensee has the right to make copies, electronic and otherwise, for the Ready To Rent course, and program development, as well as marketing to clients, landlords, and partners. Copies must be in compliance with the standards outlined below. Licensee and its instructors may not share sample curriculum with any person or entity other than internal staff, board members or at the request of funders, without consent from Ready To Rent LLC. When sharing sample curriculum, Licensee must use a "DRAFT" format and convert sample(s) to a Portable Document Format (PDF) when sending via electronic mail or any other mode of transmission. The Licensee may not sell or use any or part of the program curriculum outside of this agreement and the Ready to Rent training guidelines.
- Licensee has the liberty to translate curriculum materials into languages other than English or modify the curriculum to accommodate those with disabilities, specific state/county/city laws, and regulations, or agency/partner program guidelines. In addition, the Licensee can modify material and/or add additional curriculum material as needed to make the curriculum more effective for specific audiences.

Licensee will not be required to get approval on these curriculum changes but must provide Ready to Rent LLC with a master copy of the modified curriculum in its entirety including periodic updates. Except as otherwise provided herein, Ready To Rent LLC (copyright owner) will have a royalty free license to use all changes, modifications and derivatives of the program created by Licensee ("Derivative Works") and will credit, in writing within the curriculum, all derivative works to the Licensee.

- Licensee can add agency logo on necessary forms and marketing materials only. The "official" Ready to Rent logo must appear on all programing materials including marketing, agency website, PowerPoint slides, etc.
- Licensee will receive updates of program standards or major curriculum changes from the Ready to Rent LLC via electronic mail, the Ready To Rent cloud drive, or U.S. Mail.
- Licensee is entitled to basic on-going technical assistance via phone or e-mail.

Instructor Certification

- Instructor certification is required before teaching the Ready to Rent curriculum. To become "certified," Licensee designee(s) must complete the Instructor Certification Training prior to teaching any part of the curriculum. Certified Instructors may include staff, volunteers, board members, etc.
- All individuals teaching the Ready to Rent curriculum must complete nine (9) hours of Instructor Certification Training and sign a Certified Instructor Agreement. This training is only provided by Ready to Rent LLC via webinar. Licensee may opt for a private, on-site training for an additional cost. Instructor Certification Training includes three, 3-hour on-line sessions, teaching and marketing materials. All instructors receive basic on-going technical assistance via phone, e-mail or Zoom webinar. The cost for training is \$675 per person for all trainees under the Licensee and will not be subject to future training price increases. A previously "certified" instructor may transfer their certification to any licensed agency (unlicensed agencies must purchase a licensing from Ready To Rent LLC) and must notify Ready to Rent LLC prior to transfer.

Standards

A. Training Length

Licensee will provide class participants with the minimum training length of 12 hours. Work done outside of the class training sessions does not count towards the 12-hour total, except in cases of reasonable accommodation or makeup of a missed training session as described below.

B. Training Topics

It is the responsibility of the Licensee to assure that all six of the Ready to Rent training sessions are taught during the training series. Certified Instructors are given flexibility to give specific focus to the areas of most importance to the population being trained but must meet all training outcomes/objectives outlined in the curriculum. Additional training topic and guidelines may be added.

The training sections are:

- ✓ Training #1 Ready to Get Started
- ✓ Training #2 Ready to Solve Problems
- ✓ Training #3 Ready to Prepare Finances
- ✓ Training #4 Ready to Shop for a Home
- ✓ Training #5 Ready to Settle In
- ✓ Training #6 Ready to Move On

Limitations. Licensee will not be able to sell or distribute any portion of the Ready to Rent curriculum (including curriculum changes and alterations), the training, or any associated materials to any individual or party outside its agency.

Licensee is prohibited from making a profit on the Ready to Rent curriculum or program. If a fee-for-service must be charged, it should only be to recover the initial purchase price, Instructor Certification Provider licensing fee, or actual program and training costs.

Licensee may not teach or market the program to any party outside of the agency nor provide program consultation to any party outside of the agency without permission from Ready To Rent LLC. Licensee will forward such parties to Ready To Rent LLC before teaching, giving general program information, technical assistance, program advice or recommendations. If instruction is to be provided by the Licensee to an additional agency(s), a separate licensing agreement may be required of that agency(s) before instruction begins.

Non-Compete. The Licensee, its Certified Instructors, or any community partner(s) associated with the development, delivery, funding or promotion of Ready to Rent are prohibited from developing a similar curriculum within the first three years of a signed Licensing Agreement, once the agency or designated trainee has received materials (but did not attend or complete the Instructor Certification Training), while teaching the curriculum, or three years after discontinuation of teaching the curriculum (with the required notification to Ready To Rent LLC mentioned in "Licensing & Fee" above).

Reporting. The Licensee and Certified Instructors will periodically be asked to provide feedback on best practices developed, how the program is doing, and testimonials on the effectiveness of the program. Instructors are required to have all participants complete the "Participant Evaluation" form at the end of the course and return it to Ready To Rent LLC via U.S. mail or email. Ready To Rent LLC will provide all necessary reporting forms.

Successors and Assigns. This Licensing Agreement shall inure to the benefit of and be binding upon Ready To Rent LLC and the Licensee to the Licensing Agreement and the successors and assigns of the Licensee. Notwithstanding the foregoing, neither party may assign this Licensing Agreement without the prior written consent of the other party.

Cooperation/Further Assurances. Ready To Rent LLC and Licensee will cooperate with each other and provide such assistance as may be reasonably requested in connection with the fulfillment of their respective obligations under this Licensing Agreement.

Governing Law. This Licensing Agreement shall be governed by and construed in accordance with the laws of the State of Oregon, United States, regardless of the laws that might otherwise govern or be applicable under principles or conflicts of laws.

Enforcement/Attorney fees. The failure of either party, in one or more instances, to insist upon compliance with any of the terms and conditions or to exercise any right or privilege conferred in this Licensing Agreement shall not constitute or be construed as the waiver of such or any similar restriction, rights, options, or privilege, but the same shall continue and remain in full force and effect as if no such forbearance had occurred. This Licensing Agreement shall be enforceable by Ready To Rent LLC and the Licensee through all legal means available to comply with the Licensing Agreement and applicable rules and regulation, at law or in equity. Without limitation of available remedies, Ready To Rent LLC and the Licensee shall be entitled to injunctive relief and to demand rescission of any transaction, which was completed in violation of this Licensing Agreement. In any action commenced or taken to enforce this Licensing Agreement, Ready To Rent LLC and Licensee shall be entitled to recover reasonable attorney's fees, court costs and litigation expense incurred in connection with such enforcement action.

Time is of the Essence. Time shall be of the essence in the performance of the terms and conditions of the Licensing Agreement.

Merger. This Licensing Agreement constitutes the final, complete, and entire agreement among the parties with respect to the subject matter thereof and all prior agreements and understanding are merged herein.

Amendment. Only an instrument in writing executed by Ready To Rent LLC and the Licensee may amend the Licensing Agreement.

Severability. The invalidations of any one or more of the provisions of this Licensing Agreement or any part thereof by judgment of any court of competent jurisdiction shall not in any way affect the validity of any other provision of the Licensing Agreement, but the same shall remain in full force and effect.

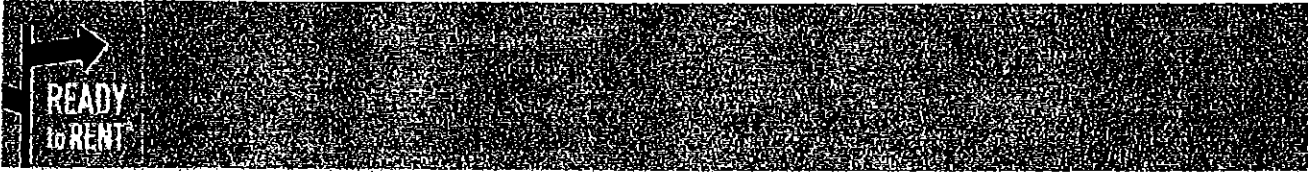
Notices. Any notices permitted or required to be given hereunder shall be given in writing and shall be delivered in person or by nationally recognized overnight courier or sent by certified mail, return receipt, postage prepaid, addressed as follows:

If to Licensor:

Ready To Rent LLC
16500 SW Walker Rd. #444
Beaverton, OR 97006

If to Licensee:

Licensee: Ohio Means Jobs Warren County
Mail Address: 300 E. Silver St
City/State/Zip: Lebanon, OH 45036



Licensing Signature Page

In Witness whereof, Ready To Rent LLC and the Licensee named below have caused this Licensing Agreement to be duly executed as of the date signed by the licensee.

Ready To Rent LLC
16500 SW Walker Rd. #444
Beaverton, OR 97006

Licensee: OhioMeansJobs Warren Co.
Address: 300 E Silver St.
City/State/Zip: Lebanon, OH 45036

By: Raina Evans
Title: Owner/Sole Proprietor
Signature: *R Evans*
Date: 02/18/2025

By: Josh Hisle
Title: DEPUTY DIRECTOR
Signature: *JH*
Date: 2.19.25

APPROVED AS TO FORM

Adam M. Nice

Adam M. Nice
Asst. Prosecuting Attorney

WARREN COUNTY COMMISSIONERS

Tom Grossmann
Tom Grossmann, President

2/25/25
Date

Resolution

Number 25-0248

Adopted Date February 25, 2025

AUTHORIZING CONTRACT AMENDMENT NO. 1 TO THE MASTER SERVICE AGREEMENT WITH ARCADIS U.S., INC. FOR THE SOUTH COVE ROADWAY IMPROVEMENT AND WATERLINE REPLACEMENT PROJECT

WHEREAS, pursuant to Resolution #24-0803, adopted June 25, 2024, this Board entered into a Master Service Agreement with Arcadis Engineering Services USA, Inc. for professional engineering and survey services on an as-needed basis; and

WHEREAS, effective January 1, 2025, Arcadis Engineering Services USA, Inc merged with Arcadis U.S., Inc. and therefore is now Arcadis U.S., Inc.; and

WHEREAS, pursuant to Resolution #25-0030, adopted January 14, 2025, this Board authorized the Warren County Sanitary Engineer to prepare and submit a final application to participate in the Ohio Public Works Commission State Capital Improvements Program for the replacement of failing waterlines; and

WHEREAS, in January 2025 the Water and Sewer Department and Deerfield Township jointly provided a scope of work to Arcadis for the replacement of waterlines along South Cove Drive and South Cove Court, roadway and drainage improvements at the intersection of South Cove and Simpson Trace, and the asphalt resurfacing of the subdivision; and

WHEREAS, on February 6, 2025, Arcadis provided the County and Township with a proposed detailed scope, schedule, and budget for surveying and the preparation of construction Contract Documents; and

WHEREAS, the County and Township have reviewed the proposal and find the work scope, schedule, and budget to be fair, reasonable, and appropriate.

NOW THEREFORE BE IT RESOLVED, to approve Contract Amendment No. 1 with Arcadis Engineering Services USA, Inc. and issue a purchase order in the amount of \$74,216.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann -- yea

Mr. Young -- yea

Mrs. Jones -- yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: c/a- Arcadis U.S., Inc
Water/Sewer (file)

Project file

**WORK ORDER CONTRACT AMENDMENT NO. 1
MASTER SERVICE AGREEMENT**

This Work Order Contract Amendment No. 1 is made and entered into effective on the date last executed by the Parties hereto, by and between the WARREN COUNTY BOARD OF COUNTY COMMISSIONERS, 406 Justice Drive, Lebanon, Ohio 45036 (hereinafter "County") and ARCADIS USA, INC., 23 Triangle Park Drive, Cincinnati, OH 45246 (hereinafter called the "Consultant").

WHEREAS, the Warren County Board of County Commissioners and Arcadis Engineering Services USA, Inc. which effective January 1, 2025, merged with Arcadis U.S., Inc. and therefore is now the legal entity of Arcadis U.S., Inc. (hereinafter "Arcadis") entered into a Master Service Agreement for Professional Consulting Services on June 25, 2024 for professional engineering and survey services on an as-needed bases; and

WHEREAS, recognizing the need to replace aged and deteriorated waterlines along South Cove Drive and South Cove Court, on January 14, 2025, the County Commissioners adopted Resolution 25-0030, authorizing the Warren County Sanitary Engineer to prepare and submit a final application to participate in the Ohio Public Works Commission State Capital Improvements Program for the replacement of the failing waterlines; and

WHEREAS, in January 2025 the Water and Sewer Department (hereinafter "County") and Deerfield Township jointly provided a scope of work to Arcadis for the replacement of waterlines along South Cove Drive and South Cove Court; roadway and drainage improvements at the intersection of South Cove and Simpson Trace; and the asphalt resurfacing of the subdivision; and

WHEREAS, on February 6, 2025, Arcadis provided the County and Township with a proposed detailed scope, schedule and budget for surveying and the preparation of construction Contract Documents; and

WHEREAS, the County and Deerfield Township will enter into an Ohio Public Works Commission Cooperation Agreement that allows for the collaborative design and construction of the improvements and partial funding through OPWC; and

WHEREAS, the County and Township have reviewed the Arcadis proposal and find the work scope, schedule, and budget to be fair, reasonable, and appropriate; and

WHEREAS, it is the recommendation of the County Sanitary Engineer to amend the Arcadis Master Service Agreement to allow for the additional professional engineering services; and

WHEREAS, it is the desire of this Board to amend said Master Service Agreement to allow for professional services including survey services and the preparation of contract documents for the replacement of waterlines along South Cove Drive and South Cove Court; roadway and drainage improvements at the intersection of South Cove and Simpson Trace; and the asphalt resurfacing of the subdivision; and

NOW, THEREFORE, IT IS AGREED by and between the County and the Consultant that the Project Agreement is hereby amended as follows:

SCOPE OF SERVICES

The contractual scope shall be modified as identified in the Consultant's proposal dated February 6, 2025, attached hereto and made a part hereof.

COUNTY RESPONSIBILITIES

The County shall supply the following data/additional services to the Consultant:

1. Provide record drawings of the existing waterlines and gravity sewers in the project area.
2. Assist Consultant by placing at their disposal all available information pertinent to the project.
3. Examine all studies, reports, sketches, drawings, proposals, and other documents presented by the Consultant, obtain advice of an attorney, insurance counselor and other consultants as deemed appropriate for such examination and render in writing decisions pertaining thereto within a reasonable time so as not to delay the service of the Consultant.

SCHEDULE

The Consultant's additional services shall commence upon the execution of this Amendment by both the Consultant and the County. Preparation of 90% design drawings for OPWC submittal shall be completed by July 14, 2025.

COMPENSATION

1. The Consultant's fee for all services performed pursuant to this Amendment shall be on a "per hour" basis for all labor incurred by the Consultant, in accordance with the June 25, 2024 Agreement.
2. Based on the scope of services as described in the Consultant's proposal dated February 6, 2025, total compensation for all additional services performed under this Amendment, and all direct reimbursable costs, shall not exceed \$74,216, including a \$3,000 allowance for the procurement of easements.
3. Payment of compensation shall be made to the Consultant within thirty (30) days after the receipt of an invoice from the Consultant.

TERMS & CONDITIONS

Except as provided herein, the June 25, 2024 Master Service Agreement shall remain binding and in force and effect in all other aspects. In the event any conflict or dispute arises between the June 25, 2024 Master Service Agreement and this Amendment No. 1, such conflict or dispute shall be resolved in accordance with the amended obligations set forth in this Amendment No. 1.

[the remainder of this page is intentionally left blank]

CONSULTANT:

IN EXECUTION WHEREOF, Arcadis Engineering Services USA, Inc. has caused this Agreement to be executed by Michael S. Murray, its Director, on the date stated below, pursuant to a corporate resolution, authorizing the same.

Arcadis USA, Inc.

SIGNATURE: 

NAME: Michael S. Murray


TITLE: Director

DATE: 2/17/25

COUNTY:

IN EXECUTION WHEREOF, the Warren County Board of Commissioners has caused this Agreement to be executed by Tom Grossmann, its President on the date stated below, pursuant to Board Resolution No. 24-0248, dated 2/25/25.

WARREN COUNTY BOARD OF
COMMISSIONERS

SIGNATURE: 

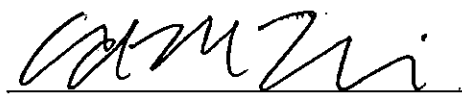
NAME: Tom Grossmann

TITLE: President

DATE: 2/25/25

Approved as to form:

DAVID P. FORNSHELL,
PROSECUTING ATTORNEY
WARREN COUNTY, OHIO



By: Adam Nice, Asst. Prosecutor



ARCADIS
8101 N High St Suite 100
Columbus OH 43235 USA
tel 614 818 4900 fax 614 881 4801
ibigroup.com

February 6, 2025

Kathryn Gilbert PE
Warren County Water and Sewer
406 Justice Drive
Lebanon, Ohio 45036

**SOUTH COVE ROADWAY IMPROVEMENT/WATER MAIN REPLACEMENT
LANDEN OH REVISED FEBRUARY 11 2025**

Dear Ms. Gilbert:

Further to our recent discussions, we are pleased to provide you (the "Client") with this Agreement for engineering services as authorized in the current 2024-2026 master agreement for professional consulting services for your project based on the information set out below.

The potential project includes replacement of the existing water line along South Cove Drive and South Cove Ct in Landen (Warren County) Oh. The project includes the replacement of approximately 3,400 LF of existing 3 inch and 6" water main with new D1 water main and appurtenances as well as the reconnection of side street mains and service line reconnects to the new main. The replacement main will be located within the right-of-way, if possible. The project will include the associated water main appurtenances, side street tie-ins, water service reconstructions, abandonment or possible removal of the existing main, and restoration.

Additionally, the project will include miscellaneous roadway and drainage improvements at the intersection of South Cove Drive and Simpson Trace and the asphalt resurfacing of the plat. The project is being developed as a joint OPWC application with Deerfield Township for the funding cycle ending in August 2025.

Arcadis US Inc. is a global team of dedicated and experienced architects, engineers, planners, designers, and technology professionals who share a common desire – to help our clients create liveable, sustainable, and advanced urban environments.

I. Surveying

- Contact OH 811/OUPS for mark-out.
- Perform boundary/topographic survey for the length of the project; locate OH 811 mark-outs; locate visible physical features, such as: trees, curbs, walks; inlets, etc.
- Establish the ROW for the purposes of engineering the project.
- Tree line will be located; however individual trees with species and caliper are not included.
- Prepare survey base plan in Civil 3D 2022.
- Distribute the drawings to utilities for confirmation.

ii. Construction Documents

- Prepare detailed construction drawings and specifications for replacement of approximately 3,400 LF of new D1 Water main along South Cove and South Cove Ct.

- Review South Cove/Simpson Trace intersection and develop a preliminary concept to add curb and improve drainage/stormwater management from the intersection along South Cove to meet existing curb.
- Develop roadway resurfacing plans for South Cove and South Cove Ct
- The Plan and profile drawings will be developed at a scale of 20H:5V.
- Review preliminary water main replacement design alignment with WCWS staff.
- Review roadway improvement plans with Deerfield Township
- Submit to all known utility companies, Warren County Engineer Office and Deerfield Township Service Dept and Fire Dept for comment/review of utility location, ownership, and information on potential upcoming projects in the area.
- Complete final design of the proposed water main improvements including:
 - Service reconnects.
 - Side road connections and details
 - Review/reset/ fire hydrant locations.
- Complete final design of the proposed roadway improvements including.
 - Roadway Typical Section
 - General Notes
 - South Cove/Simpson Trace plan and profile with storm sewer and curb improvements
 - South Cove Cross Sections
 - South Cove/Simpson Trace Storm Sewer Profile
 - South Cove/Simpson Trace intersection detail
 - Calculate Pavement Sub summary
 - Maintenance of Traffic
 - Develop a General Summary with quantity splits by jurisdiction
- Develop an opinion of anticipated construction cost estimate
- Attend one (1) resident coordination meeting. Prepare exhibits and assist with project presentation to the residents.
- Prepare any required easements (legal descriptions and exhibits – assume maximum of 3) per Warren County Requirements if authorized by WCWS
- Assist with the procurement of all required permits and approvals;
- Complete As built drawings based on field verification and information provided by WCWS staff
- Final deliverables will include
 - Signed/sealed construction drawings
 - Final Opinion of Construction cost estimate w/ quantity splits
 - As built record drawings

For this project, we have made the following assumptions:

1. Once started, the design will move forward through completion. Delays of 4 months or more may require our team to re-evaluate the scope of work, schedule and fee.
2. Any revisions/ modifications that are requested during the course of design or construction that are a result of client changes in direction or layout are not included. However, if revisions are necessary, we will discuss the change in the scope of services and determine a fee for the additional services at that time.
3. We have assumed up to 3 meetings with WCWS and Deerfield Township staff to coordinate the project deliverables and review comments, phasing etc.
4. Arcadis will not be responsible to obtain permits or right of entries to private property.
5. It is assumed all work will be in the ROW or an existing easement and plats, easement exhibits and legal descriptions; however, we have assumed a maximum of 3 easements if necessary. Recording of easements will be by owner
6. Arcadis will assist with the preparation and submission of the NOI permit if required. We are assuming an EPA PTI for the water main is not required. All fees shall be paid directly by WCWS and/or Deerfield Township. Any other permits (such as USACE 401, OEPA 404, etc.) determined to

be needed during the development of the project will be completed following the approval of additional scope of services and price.

7. This proposal includes obtaining plan approvals for the construction plans identified in our Scope of Services but does not include costs associated with obtaining construction/Contractor Permits.
8. Our scope of work does not include the preparation of bid documents, construction administration and inspection but a scope of work and price proposal can be provided if requested. We have assumed the County/Township will complete bidding and construction, but ARCADIS will be available during the duration of the project to respond to bidder/contractor questions that cannot be fielded by the Client.
9. This proposal does not include the design of any utility relocations
10. Our scope/price does not include geotechnical engineering, sanitary sewer replacement or repair, environmental permitting, and stormwater and/or roadway improvements outside of the work outlined above.
11. Our scope assumes a single set of plans to be developed with quantity splits for items assigned to WCWS and Deerfield Township

2. Your Schedule

Upon receipt of the signed contract, we can get started immediately. We anticipate our survey team can be in the field within 2 weeks of authorization. Assumed Authorization Date of March 3, 2025

Anticipated Task Duration

Survey and Base mapping – 2 weeks Complete by March 31, 2025

Preliminary Design (50%) – 6 weeks Complete by May 12, 2025

County/Township Review – 2 weeks Complete by May 26, 2025

Final Design/Draft OPWC Submittal (90%) – 8 weeks Complete by July 14, 2025

County/Township Review – 2 weeks Complete by July 28, 2025

OPWC Revised Submittal – 2 weeks Complete by August 11, 2025

Construction Drawings – 6 weeks Complete by September 22, 2025

Resident Coordination Meeting – October 2025

Bidding – Winter 2026

Commence Construction July 2026

As built Documents Fall/Winter 2026

We are confident we can deliver a complete set of plans with an opinion of construction cost estimate for inclusion in an OPWC application prior to the September 2025, deadline.

Payment

Based on the MSA Schedule you will pay us on the following Not to Exceed basis of \$71,216 per the contract regulations.

If Authorized: Easement preparation - \$1,000/easement (Assumes max of 3)

We invoice for payment monthly. Thereafter, payment is due within thirty (30) days of your receipt of our invoice.

We look forward to working with you. Should you have any questions about the materials presented, or need additional information, please do not hesitate to contact Mike Murray at (513) 509-9336.

Yours truly,

Arcadis US Inc.



Name: Mike Murray

Title: Director

If this accurately sets out our understanding and is acceptable to you, please indicate your agreement by signing in the space below.

Agreed to and accepted effective the date of this Agreement.

Warren County Water and Sewer

By: 

Name: Tom Grossmann

Title: President

Resolution

Number 25-0249

Adopted Date February 25, 2025

ACKNOWLEDGING PAYMENT OF BILLS

BE IT RESOLVED, to acknowledge payment of bills from 2/18/25 and 2/25/25 as attached hereto and made a part hereof.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

/kp

cc:

Auditor ✓

Resolution

Number 25-0250

Adopted Date February 25, 2025

APPROVING VARIOUS RECORD PLATS

BE IT RESOLVED, upon recommendation of the Warren County Regional Planning Commission, to approve the following Record Plats:

- Fein Subdivision Replat – Deerfield Township

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Plat File
RPC

Resolution

Number 25-0251

Adopted Date February 25, 2025

CREATING THE BETHANY & HUDSON HILLS ROAD PROJECT FUND #4427,
ACCEPTING AN AMENDED CERTIFICATE FOR FUND #4427 AND APPROVING A
SUPPLEMENTAL APPROPRIATION AND A CASH ADVANCE INTO FUND #4427

WHEREAS, in order for the Warren County Engineer's Office to be able to encumber funds for the Bethany & Hudson Hills Road Project, the creation of fund #4427, an amended certificate, a supplemental appropriation, and a cash advance are necessary.

NOW THEREFORE BE IT RESOLVED, to approve creation of fund #4427, and accept an amended certificate from the Budget Commission in the amount of \$321,670.00 for the Bethany and Hudson Hills Road Project; and

BE IT FURTHER RESOLVED, to approve the following supplemental appropriation and cash advance for the Engineer's Fund #4427:

Supplemental Appropriation

\$321,670.00 into #44273120-5320 (Capital Purchases)

Cash Advance

\$321,670.00 from #2202-45556 (Advances of Cash Out)
 into #4427-45555 (Cash Advance In)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS


Ashley Watts, Deputy Clerk

cc: Auditor ✓
Amended Certificate file
Supplemental App. file
Engineer (file)

AMENDED OFFICIAL CERTIFICATE OF ESTIMATED RESOURCES

Rev. Code , Sec 5705.36

Office of Budget Commission, County of Warren, Lebanon, Ohio, February 21, 2025

To the TAXING AUTHORITY of Warren County Commissioners

The following is the amended certificate of estimated resources for the fiscal year beginning January 1st, 2025, as revised by the Budget Commission of said county, which shall govern the total of appropriations made at any time during such fiscal year.

FUND TYPE - Capital Projects	Jan. 1st, 2025	Taxes	Other Sources	Total
Bethany & Hudson Hills Rd Proj	\$0.00		\$321,670.00	\$321,670.00
Fund 4427				
TOTAL	\$0.00	\$0.00	\$321,670.00	\$321,670.00

_____)
 _____)
Matt Nolan BO)
 _____) Budget
 _____) Commission

AMEND 25 04
Fund 4427+321,670.00

Resolution

Number 25-0252

Adopted Date February 25, 2025

APPROVING A SUPPLEMENTAL APPROPRIATION INTO CLERK OF COURTS FUND
#2282

BE IT RESOLVED, to approve the following supplemental appropriation:

\$56,100.00 into #22821410-5370 (Software Non-Date Board)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

/sz

cc: Auditor
Supplemental App. File
Clerk of Courts (file)

Resolution

Number 25-0253

Adopted Date February 25, 2025

APPROVING A SUPPLEMENTAL APPROPRIATION INTO COMMON PLEAS COURT
COMMUNITY BASED CORRECTIONS FUND #2289

BE IT RESOLVED, to approve the following supplemental appropriation:

\$ 5,000.00 into BUDGET-BUDGET #22891223-5910 (Other Expense)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor ✓
Supplemental Appropriation file
Common Pleas (file)

Resolution

Number 25-0254

Adopted Date February 25, 2025

APPROVING A SUPPLEMENTAL APPROPRIATION INTO COMMON PLEAS COURT
COMMUNITY BASED CORRECTIONS #2289

BE IT RESOLVED, to approve the following supplemental appropriation:

\$ 4,000.00 into BUDGET-BUDGET #22891223-5317 (Non Capital Purchases)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

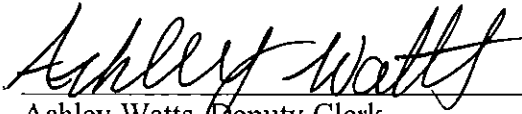
Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Supplemental Appropriation file
Common Pleas (file)

Resolution

Number 25-0255

Adopted Date February 25, 2025

APPROVING AN APPROPRIATION ADJUSTMENT WITHIN ECONOMIC
DEVELOPMENT FUND #11011116

BE IT RESOLVED, to approve the following appropriation adjustment:

\$100.00 from #11011116-5910 (Econ Dev Other Expense)
 into #11011116-5911 (Econ Dev Non Taxable Meal Fringe)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea


Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

AW/

cc: Auditor 
Appropriation Adjustment file
Economic Development (file)

Resolution

Number 25-0256

Adopted Date February 25, 2025

APPROVING AN APPROPRIATION ADJUSTMENT WITHIN FACILITIES
MANAGEMENT FUND #11011600

BE IT RESOLVED, to approve the following appropriation adjustment:

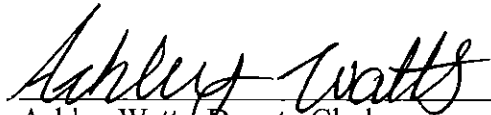
\$70.00	from	#11011600-5210	(Materials & Supplies)
	into	#11011600-5830	(Workers Compensation)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Appropriation Adj. file
Facilities Management (file)

Resolution

Number 25-0257

Adopted Date February 25, 2025

APPROVING AN APPROPRIATION ADJUSTMENT WITHIN COMMON PLEAS COURT
FUND #11011223

BE IT RESOLVED, to approve the following appropriation adjustment:

\$20,000.00 from #11011223-5820 (Health & Life Insurance)
into #11011223-5830 (Workers Comp)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Appropriation Adjustment file
Common Pleas Court (file)

Resolution

Number 25-0258

Adopted Date February 25, 2025

APPROVING AN APPROPRIATION ADJUSTMENT WITHIN SHERIFF'S OFFICE FUND
#11012210

BE IT RESOLVED, to approve the following appropriation adjustment within Warren County
Sheriff's Office Fund #1101:

\$6,599.99 from #11012210 5400 (Purchased Services)
 into #11012210 5830 (Worker's Comp)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon
call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
 Appropriation Adjustment file
 Sheriff's Office (file)

Resolution

Number 25-0259

Adopted Date February 25, 2025

APPROVING APPROPRIATION ADJUSTMENTS FROM JUVENILE COURT DETENTION CENTER FUND #11012600 INTO JUVENILE COURT DETENTION CENTER FUND #11012600 AND JUVENILE PROBATION FUND #11012500

BE IT RESOLVED, to approve the following appropriation adjustments:

\$7,000.00 from #11012600-5102 (Juv. Det. Center – Regular Salaries)
into #11012600-5830 (Juv. Det. Center – Workers Comp.)

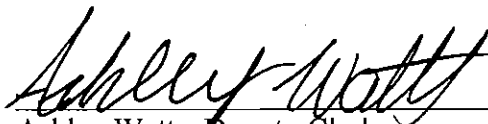
\$7,000.00 from #11012600-5102 (Juv. Det. Center – Regular Salaries)
into #11012500-5830 (Juvenile Probation – Workers Comp.)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Appropriation Adj. file
Juvenile (file)

Resolution

Number 25-0260

Adopted Date February 25, 2024

APPROVING APPROPRIATION ADJUSTMENTS WITHIN VETERANS FUND #11015220

BE IT RESOLVED, to approve the following appropriation adjustment:

\$60,386.40	from	#11015220-5920	(Vet SRelief Allowances)
	into	#11015210-5830	(Vet Admin Workers Compensation)
\$ 1,000.00	from	#11015220-5920	(Vet SRelief Allowances)
	into	#11015220-5871	(Medicare)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Appropriation Adj. file
Veterans (file)

Resolution

Number 25-0261

Adopted Date February 25, 2025

APPROVING APPROPRIATION ADJUSTMENTS WITHIN HUMAN SERVICES FUND
#2203

BE IT RESOLVED, to approve the following appropriation adjustments within Human Services fund #2203:

\$180,000.00	from	#22035310-5749	(Children Services)
\$136,000.00	into	#22035310-5102	(Regular Salaries)
\$ 19,000.00	into	#22035310-5811	(PERS)
\$ 23,000.00	into	#22035310-5820	(Health & Life Insurance)
\$ 2,000.00	into	#22035310-5871	(Medicare)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Appropriation Adjustment file
Human Services (file)

Resolution

Number 25-0262

Adopted Date February 25, 2025

APPROVING AN APPROPRIATION ADJUSTMENT WITHIN EMERGENCY SERVICES /
EMERGENCY MANAGEMENT FUND #2264

BE IT RESOLVED, to approve the following appropriation adjustment:

\$921.87	from	#22642800-5102	(Regular Salaries)
	into	#22642800-5830	(Workers Compensation)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

cc: Auditor
Appropriation Adjustment file
Emergency Services (file)

Resolution

Number 25-0263

Adopted Date February 25, 2025

APPROVING APPROPRIATION ADJUSTMENTS WITHIN SOLID WASTE FUND #2256
AND COMMUNITY DEVELOPMENT FUND #2265

BE IT RESOLVED, to approve the following appropriation adjustments:

\$184.57 from #22564410-5210 (Material & Supplies)
 into #22564410-5830 (Workers Compensation)

\$914.37 from 22653410-5910 (Other Expense)
 into 22653410-5830 (Workers Compensation)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea
Mr. Young – yea
Mrs. Jones – yea

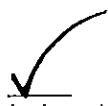
Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

/sh

cc: Auditor 
Appropriation Adj. file
Grants (file)
Solid Waste (file)

Resolution

Number 25-0264

Adopted Date February 25, 2025

APPROVING AN APPROPRIATION ADJUSTMENT WITHIN THE WATER REVENUE FUND #5510

WHEREAS, the Water and Sewer Department incurs costs pertaining to Workers Compensation; and

WHEREAS, an appropriation adjustment is necessary to accommodate said costs.

NOW THEREFORE BE IT RESOLVED, to approve the following appropriation adjustment:

\$114.14	from	55103200 - 5998	(Reserve/Contingency)
	into	55103200 - 5830	(Workers Compensation)

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

mbz

cc: Auditor
Appropriation Adj. file
Water/Sewer (file)

Resolution

Number 25-0265

Adopted Date February 25, 2025

APPROVING REQUISITIONS AND AUTHORIZING THE COUNTY ADMINISTRATOR
TO SIGN DOCUMENTS RELATIVE THERETO

BE IT RESOLVED, to approve requisitions as listed in the attached document and authorize
Martin Russell, County Administrator, to sign on behalf of this Board of County Commissioners.

Mrs. Jones moved for adoption of the foregoing resolution being seconded by Mr. Young. Upon
call of the roll, the following vote resulted:

Mr. Grossmann – yea

Mr. Young – yea

Mrs. Jones – yea

Resolution adopted this 25th day of February 2025.

BOARD OF COUNTY COMMISSIONERS



Ashley Watts, Deputy Clerk

/kp

cc:

Commissioners' file

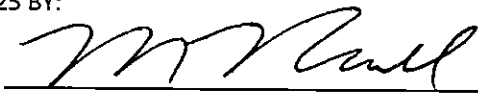
REQUISITIONS

Department	Vendor Name	Description	Amount
WAT	ARCADIS ENGINEERING SERVICES (USA) INC	WAT CB SOUTH COVE WTRMN REPL &	\$ 74,216.00 *capital purchase/ contract in packet
WAT	RODOC LEASING SALES & SERVICE LLC	WAT SURE- TRAC HEAVY EQUIPMENT	\$ 17,965.00 *capital purchase/ 3 quotes

PO CHANGE

FAC	DEBRA KUEMPEL INC	FAC DOOR ACCESS CONTROLS	\$ 12,900.00 *increase
-----	-------------------	--------------------------	------------------------

APPROVED 2/25/25 BY:



Martin Russell, County Administrator