



**BOARD OF COUNTY COMMISSIONERS
WARREN COUNTY, OHIO**

406 Justice Drive, Lebanon, Ohio 45036

www.co.warren.oh.us

commissioners@co.warren.oh.us

Telephone (513) 695-1250

Facsimile (513) 695-2054

TOM GROSSMANN

SHANNON JONES

DAVID G. YOUNG

GENERAL SESSION AGENDA

May 2, 2023

- #1** **Clerk — General**
- #2** **9:00** **Warren County Investment Advisory Board Meeting**
- #3** **9:15** **Work Session — Tammy Whitaker, Benefits Administrator, to Present
HIPAA Privacy and Security Policies and Procedures for Warren
County Organized Health Care Arrangements**
- #4** **9:30** **Work Session — Trevor Hearn, Director of Facilities Management,
Relative to Campus Master Plan Study**
- #5** **10:00** **Executive Session —Conference with the Board's Legal Counsel
Concerning Disputes that are Subject of Pending and Imminent Court
Action Pursuant to ORC 121.22(G)(3)**

The Board of Commissioners' public meetings can now be streamed live at [Warren County Board of Commissioners - YouTube](#)

APPROVE REQUISITIONS AND AUTHORIZE COUNTY ADMINISTRATOR TO SIGN DOCUMENTS RELATIVE THERETO

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

M moved for adoption of the foregoing resolution being seconded by M. Upon call of the roll, the following vote resulted:

M
M
M

Resolution adopted this 2nd day of May 2023.

BOARD OF COUNTY COMMISSIONERS

Tina Osborne, Clerk

/tao

cc:

Commissioners' file

REQUISITIONS

Department	Vendor Name	Description	Amount
BLD	CINCYAUTOS INC	BLD FORD EXPLORER XLT 4WD. 2.3	\$ 39,220.00
TEL	GEN CORE CANDEO LTD	TEL- "RENEWAL" GENWATCH RADIO	\$ 9,889.00

PO CHANGE ORDER

ENG	EAGLE BRIDGE	KING AVE BRIDGE PROJECT	\$ 695,781.44 DECREASE
-----	--------------	-------------------------	------------------------

5/2/2023 APPROVED:

Tiffany Zindel, County Administrator

CONSENT AGENDA*

May 2, 2023

Approve the minutes of the April 25, 2023, Commissioners' Meeting.

PERSONNEL

- 1. Hire Emily Harris as Administrative Clerk and Rachel McAninch as On-Going Caseworker II within Children Services*
- 2. Accept resignation of Jessica Anderson, Eligibility Referral Specialist II within Human Services*
- 3. Approve end of probationary period and pay increase for Tyler Blair within Telecomm*
- 4. Approve pay increase for Sara Orr within Emergency Services*
- 5. Approve internal posting of "Water Distribution/Customer Service Worker" and "Water Distribution/New Construction Locator" within Water/Sewer Department*

GENERAL

- 6. Approve reappointment of Sharon Woodrow to the Mental Health Recovery Services of Warren and Clinton Counties Board of Directors*
- 7. Approve liquor permit application for event at Warren County Fairgrounds*
- 8. Enter into agreement with Board of Developmental Disabilities and Warren County Transit*
- 9. Authorize Telecommunications to accept transfer of surplus radios from Turtlecreek Township*
- 10. Enter into annual renewal and maintenance agreement with Gencore Candeo, LTD on behalf of Telecommunications*
- 11. Approve MOU between Children Services and Warren County Recovery Court*
- 12. Approve various provider agreement on behalf of Children Services*
- 13. Declare various items as surplus and authorize disposal through internet auction*
- 14. Acknowledge payment of bills*
- 15. Approve W/S performance bond release for Grand Communities LLC*
- 16. Approve final plat*

FINANCIAL

- 17. Approve supplemental appropriation into Community Corrections 2227*
- 18. Approve appropriation adjustment from Commissioners 11011110 into Sheriff 11.12210 for payout*
- 19. Approve appropriation adjustments within OMB 11011115 and Juvenile Court 2247*

**Please contact the Commissioners' Office at (513) 695-1250 for additional information or questions on any of the items listed on the Consent Agenda*



**BOARD OF COUNTY COMMISSIONERS
WARREN COUNTY, OHIO**

406 Justice Drive, Lebanon, Ohio 45036

www.co.warren.oh.us

commissioners@co.warren.oh.us

Telephone (513) 695-1250

Facsimile (513) 695-2054

***TOM GROSSMANN
SHANNON JONES
DAVID G. YOUNG***

**BOARD OF COUNTY COMMISSIONERS
WARREN COUNTY, OHIO**

MINUTES: Regular Session – April 25, 2023

This is a summary of actions and discussions of the meeting. You may view this meeting through our YouTube Channel at <https://www.youtube.com/channel/UC1ELh0jGpXd4VV2DTgsuqPA> or by contacting our office.

The Board met in regular session pursuant to adjournment of the April 18, 2023, meeting.

Shannon Jones – present

Tom Grossmann – present

David G. Young – present

Tina Osborne, Clerk – present

Minutes of the April 18, 2023 meeting were read and approved.

- 23-0498 A resolution was adopted to approve end of 365-day probationary period and approve a pay increase for David Edwards within the Warren County Garage. Vote: Unanimous
- 23-0499 A resolution was adopted to adopt classifications specifications and point factor assignments of Water Distribution, Customer Services Worker within the Water and Sewer Department. Vote: Unanimous
- 23-0500 A resolution was adopted to adopt classifications specifications and point factor assignments of Water Distribution/ New Construction Locator within the Water and Sewer Department. Vote: Unanimous
- 23-0501 A resolution was adopted to hire Kaitlyn Niles as Emergency Communications Operator within the Warren County Emergency Services Department. Vote: Unanimous
- 23-0502 A resolution was adopted to remove probationary employee Ashley Vagedes, within the Department of Job and Family Services, Children Services Division. Vote: Unanimous

- 23-0503 A resolution was adopted to approve promotion of Dusty Johnson from Building and Electrical Inspector III to Residential Building Official within the Building and Zoning Department. Vote: Unanimous
- 23-0504 A resolution was adopted to approve amendment to Work Rules relative to the Warren County Emergency Services and the Emergency Communications Operators. Vote: Unanimous
- 23-0505 A resolution was adopted to approve departmental work rules relative to the Warren County Emergency Management Agency. Vote: Unanimous
- 23-0506 A resolution was adopted to set public hearing concerning proposed amendments to the Warren County Subdivision Regulations. Vote: Unanimous
- 23-0507 A resolution was adopted to set public hearing to consider amendments to the Warren County Official Thoroughfare Plan. Vote: Unanimous
- 23-0508 A resolution was adopted to approve emergency electric motor replacement at Lower Little Miami Waste Water Treatment Plant. Vote: Unanimous
- 23-0509 A resolution was adopted to advertise for bids for the Moreland Acres Water Main Replacement Project. Vote: Unanimous
- 23-0510 A resolution was adopted to authorize Request for Proposals for Non-Emergency Transportation Services (NET) for Warren County Medicaid Consumers. Vote: Unanimous
- 23-0511 A resolution was adopted to approve Notice of Intent to award bid to Stauffer Site Services LLC for the State Route 73 at Corwin Road Forcemain Relocation Project Re-Bid. Vote: Unanimous
- 23-0512 A resolution was adopted to award the bid to Mt. Orab CDJR for the purchase of two handicap upfit 2023 Chrysler Voyager LX vans and two standard 2023 Chrysler Voyager LX vans. Vote: Unanimous
- 23-0513 A resolution was adopted to authorize the President of the Board to enter into a joint agreement with the Hamilton County Board of Commissioners for the Fields Ertel Road Widening Project on behalf of the Warren County Engineer's Office. Vote: Unanimous
- 23-0514 A resolution was adopted to approve agreements and addendums with various providers relative to home placement and related services on behalf of Warren County Children Services. Vote: Unanimous
- 23-0515 A resolution was adopted to acknowledge payment of bills. Vote: Unanimous
- 23-0516 A resolution was adopted to approve a subdivision public improvement performance and maintenance security agreement release with M/I Homes of Cincinnati, LLC for Auburn Grove, situated in the City of South Lebanon. Vote: Unanimous

- 23-0517 A resolution was adopted to enter into a subdivision public improvement performance and maintenance security agreement with the Union Village Development Company, LLC for installation of certain improvements in Union Village, Phase 1C and 1D situated in Turtlecreek Township. Vote: Unanimous
- 23-0518 A resolution was adopted to enter into street and appurtenances (including sidewalks) security agreement with Union Village Development Company for installation of certain improvements in Union Village, Phase 1C and Phase 1D situated in Turtlecreek Township. Vote: Unanimous
- 23-0519 A resolution was adopted to approve various record plats. Vote: Unanimous
- 23-0520 A resolution was adopted to approve appropriation adjustment within Facilities Management #11011600. Vote: Unanimous
- 23-0521 A resolution was adopted to approve appropriation adjustment within the Building and Zoning Department Fund #11012300. Vote: Unanimous
- 23-0522 A resolution was adopted to approve appropriation adjustment within Workforce Investment Board Fund #2238. Vote: Unanimous
- 23-0523 A resolution was adopted to approve appropriation adjustment within Children Services Fund #2273. Vote: Unanimous
- 23-0524 A resolution was adopted to approve appropriation adjustment within Telecommunications Department Fund #4492. Vote: Unanimous
- 23-0525 A resolution was adopted to approve appropriation adjustment within the Water Revenue Fund #5510. Vote: Unanimous
- 23-0526 A resolution was adopted to approve requisitions and authorize County Administrator to sign documents relative thereto. Vote: Unanimous
- 23-0527 A resolution was adopted to cancel the regularly scheduled Commissioners' Meeting of Thursday, April 27, 2023. Vote: Unanimous
- 23-0528 A resolution was adopted to approve lease agreements with Ohio Department of Public Safety relative to 19 Dave Avenue Lebanon, Ohio. Vote: Unanimous

DISCUSSIONS

On motion, upon unanimous call of the roll, the Board accepted and approved the consent agenda.

Mary Huttlinger, Government Affairs Director of the Realtor Alliance Greater Cincinnati, was present to introduce herself and presented the attached PowerPoint Presentation.

Ms. Huttlinger explained who the Realtor Alliance is and the various ways to partner with the community.

Michelle Teigtmeier, Building and Zoning Director, was present along with Anna Helton, Office Administrator, for a work session to discuss fee waivers from non-profit organizations.

Mrs. Helton presented the attached PowerPoint presentation, reviewing the policy relative to fee waivers for political subdivisions relative to building permit fee waivers as well as a request to consider a proposed policy for zoning permit fee waiver requests. She then requested the Board to consider the request to consider the same policies for non-profit organizations as they currently do political subdivisions.

There was discussion relative to how to determine who would qualify for the waiver.

There was discussion relative to the political subdivision policy being taxpayer money vs. a non-profit request as well as the current method of having the ability to decide a fee waiver request on a case-by-case basis.

Upon discussion, the Board determined to continue with the practice of considering each request on an individual basis.

Trevor Hearn, Facilities Management Director, was present for a continuation of the discussion regarding the Warren County Campus Master Plan.

Mr. Hearn stated his desire to focus on Phase 1 of the plan and presented the attached PowerPoint presentation reviewing the existing campus, Phase 1A to demolish the Old Jail and SWAT Garage and construct a new SWAT Garage offsite.

Mr. Hearn reviewed Phase 1B to construct the new County Court Building and adjacent parking lot and then demolish the existing County Court building. He stated the possibility of some cost savings should the Board determine to proceed with Phase 1C to construct a new Facilities Management Building and parking lot on the site of the demolished Old Jail and County Court location by combining the project into one Design/Build project.

There was much discussion relative to the proposed location of the proposed new County Court Building vs. building a multi-story addition to the Common Pleas Court.

Commissioner Jones stated that the courts have been patient and it is not her desire to delay this any longer.

Mr. Hearn reviewed the history of the process relative to the various studies that have been completed.

There was discussion on the recommendation to demolish the current Health and Human Services Building.

Upon further discussion, the Board requested Mr. Hearn to schedule a work session with the architect present in order to discuss the County Court building location.

Terrell Richardson, Pet Partners Animal Therapy, was present along with members from the organization and their pets, to receive the proclamation to proclaim April 30, 2023, as "National Pet Therapy Day" in Warren County.

On motion, upon unanimous call of the roll, the Board entered executive session at 10:15 a.m. to discuss disputes involving the Board that are subject to pending litigation with legal counsel present pursuant to Ohio Revised Code Section 121.22 (G)(3) and exited at 11:09 a.m.

Upon motion the meeting was adjourned.

Shannon Jones, President

David G. Young

Tom Grossmann

I hereby certify that the foregoing is a true and correct copy of the minutes of the meeting of the Board of County Commissioners held on April 25, 2023, in compliance with Section 121.22 O.R.C.

Tina Osborne, Clerk
Board of County Commissioners
Warren County, Ohio



REALTOR® ALLIANCE *of*
GREATER CINCINNATI

Warren County

Mary Huttlinger
Director of Government Affairs

<https://cincyrealtoralliance.com/>





Who We Are



The REALTOR® Alliance of Greater Cincinnati (RAGC) is **one of the oldest REALTOR® Associations in the country.**

One of the original six local real estate boards started the National Association of REALTORS® (NAR).

RAGC currently **represents over 6,000 active REALTOR® members** through continuing education, community involvement, and advocacy.

We represent **1,081 REALTOR®** members in Warren County.

<https://cincyrealtoralliance.com/>



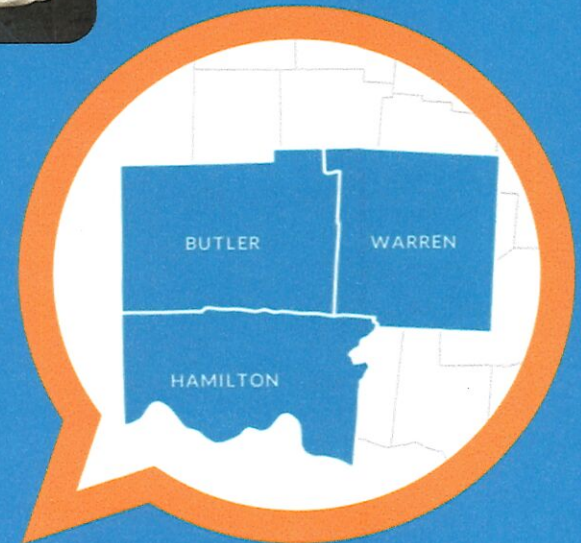


Who We Are

REALTORS® are licensed real estate agents who are members of the National Association of REALTORS® (NAR), the **largest trade group in the country**. Every real estate agent is not a REALTOR®, but most are.

REALTORS® are held to **a higher ethical standard** than real estate agents and must adhere to a stringent REALTOR® Code of Ethics.

<https://cincyrealtoralliance.com/>





REALTOR® ALLIANCE of
GREATER CINCINNATI

Who We Are

RAGC fosters inclusive member and community relationships by advocating for **equal housing opportunities, property rights, homeownership, real estate investment, and economic vitality**, and delivers education to uphold the highest professional standards that empower our members to thrive.



<https://cincyrealtoralliance.com/>



Who We Are

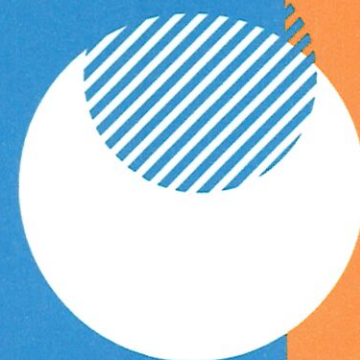


RAGC consists of a full time team of association professionals and volunteer leaders, who serve as **subject matter experts**, working collectively to advance the REALTOR® profession.

RAGC **champions real estate** and enhances the success of those we serve by focusing on connections, advocacy, and professionalism.

RAGC is a **full-service professional association** dedicated to advancing the REALTOR® profession, it also is the parent organization for CincyMLS (Cincinnati Multiple Listing Service).

<https://cincyrealtoralliance.com/>





REALTOR® ALLIANCE of
GREATER CINCINNATI

ECONOMIC IMPACT

<https://cincyrealtoralliance.com/>



\$5.8 Billion

2022 residential real estate sales of over \$5.8 billion have a major economic impact on the Greater Cincinnati area.



14.6%

The real estate industry accounts for roughly 14.6% of Ohio's gross state product (2021).



1-2 Ohio Jobs

Every home sale directly supports 1-2 jobs in Ohio with an average annual salary of \$51,200.



\$241,800

Each home sale at the median price range, \$241,800, generates roughly \$72,800 of direct local economic impact.



\$12,000

Each real estate sale triggers an average of \$12,000 in multiplier expenditures, benefitting ancillary industries.



3,500

Average monthly residential real estate transactions in Hamilton, Butler, and Warren counties.



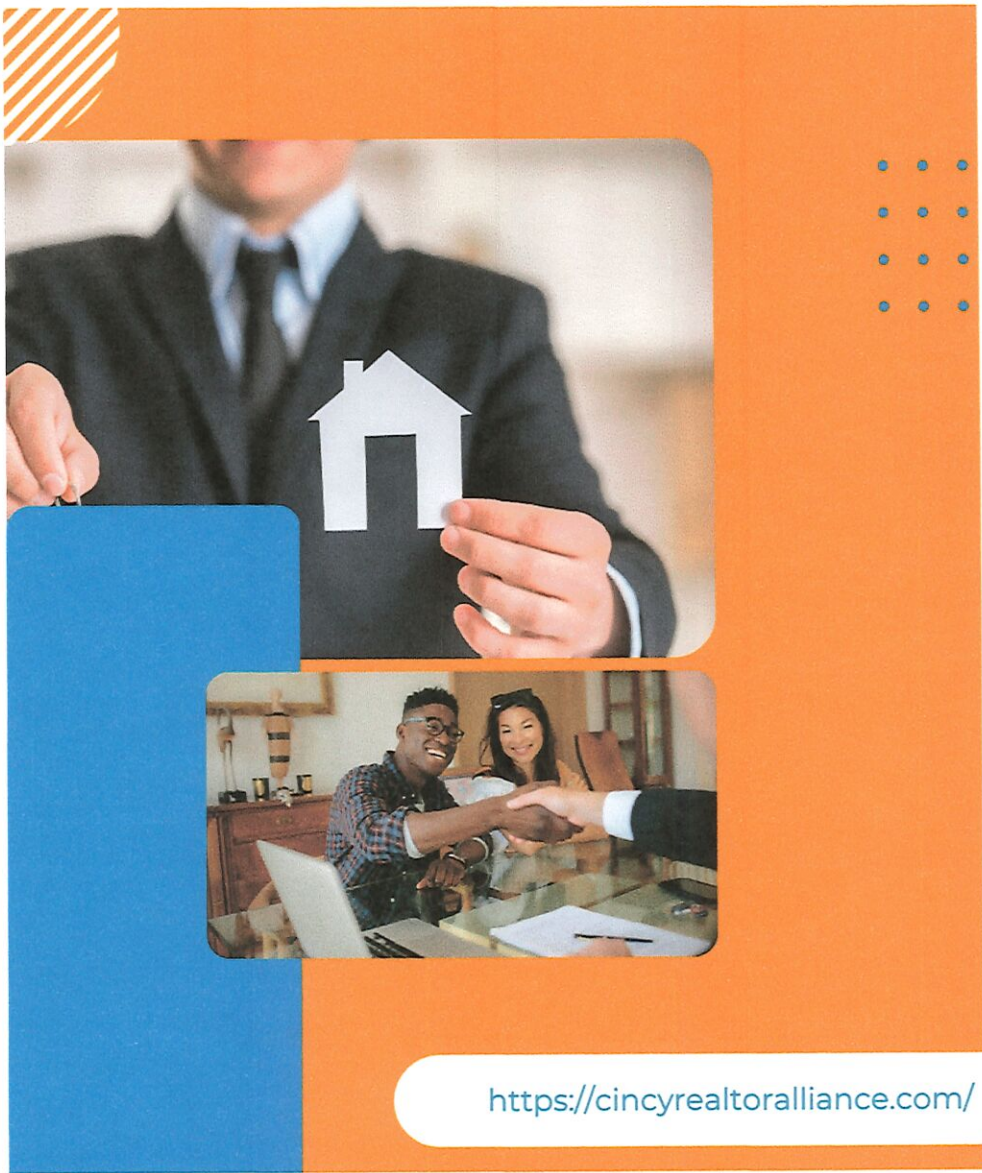
17%

Real estate transactions account for 17% of the US GDP and is a major driver of the US economy.



\$107.7 Billion

The real estate industry accounts for roughly \$107.7 billion of the US GDP.



<https://cincyrealtoralliance.com/>

Community Grants

REALTORS® are committed to collaborating with other community leaders and elected officials to **build better communities.**

- Affordable Housing
- Fair Housing
- Community Planning & Development
- Placemaking
- Rural-related Advocacy

As subject matter experts, we take pride in helping our leaders craft **custom solutions to housing challenges.**

Ask us how we can help you!



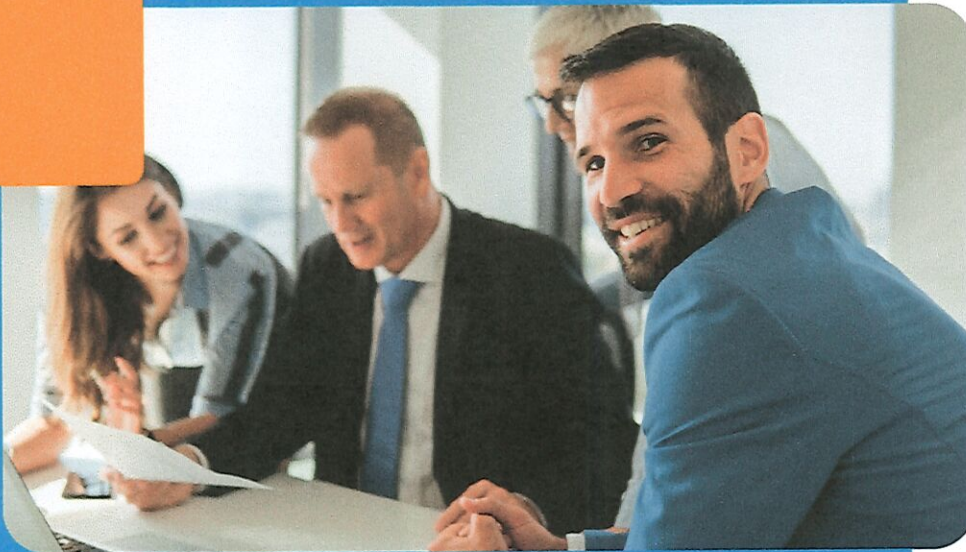
MODERN GROWTH MANAGEMENT

The Growth Management Fact Book provides a comprehensive look at **modern growth management techniques**, such as urban growth boundaries, housing moratoria, adequate public facilities and cluster zoning.

Ideas to develop well-reasoned policy positions to help advance growth-related issue priorities.

Includes the latest on parking reform trends, planning for equity models, missing middle housing strategies.

Ask us for a copy or to host a roundtable discussion!



<https://cincyrealtoralliance.com/>



REALTOR® ALLIANCE of
GREATER CINCINNATI



Ohio REALTORS® & UC Research Study on Workforce Housing

- Ohio has a **shortage of 252,027** affordable rental homes
- Affordable housing plays a very important role in our economic growth and the future of our great state
- Production of two-to-four-unit structures, likely considered workforce housing, **fell by nearly 75%** during the last two decades
- This comprehensive study provides a **critically important framework** for understanding this challenge so we can begin to address it through smart policy initiatives.
- **ASK US for a copy!**

<https://cincyrealtoralliance.com/>





REALTOR® ALLIANCE *of*
GREATER CINCINNATI

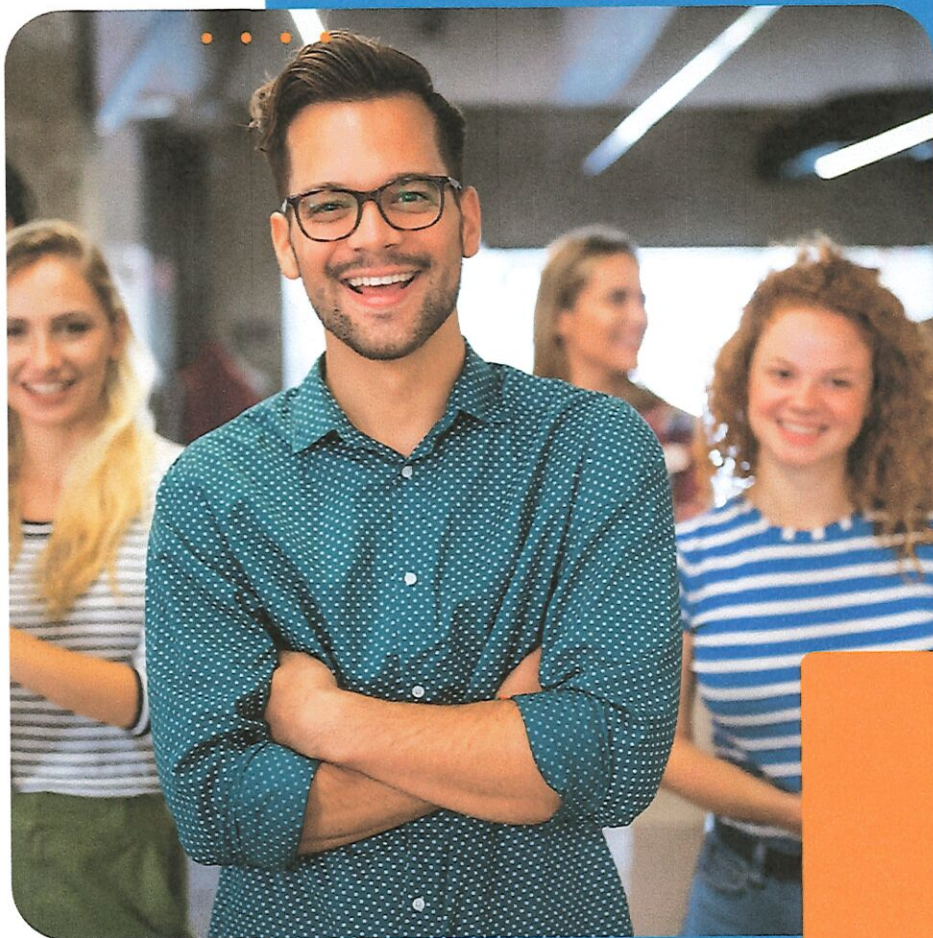


Current REALTOR® Issues

We work hard to serve our communities, and track **best practices** across the country. Lean on us for viable solutions to:

- Housing Inventories
- Affordable Housing
- Smart Development
- Property Taxes
- Alternative Housing - ADUs
- Institutional Investors
- Tax Abatement

<https://cincyrealtoralliance.com/>



Partner with Us

Stay in touch, let us be your subject matter experts!

Thank you.

Mary Huttlinger

Director of Government Affairs

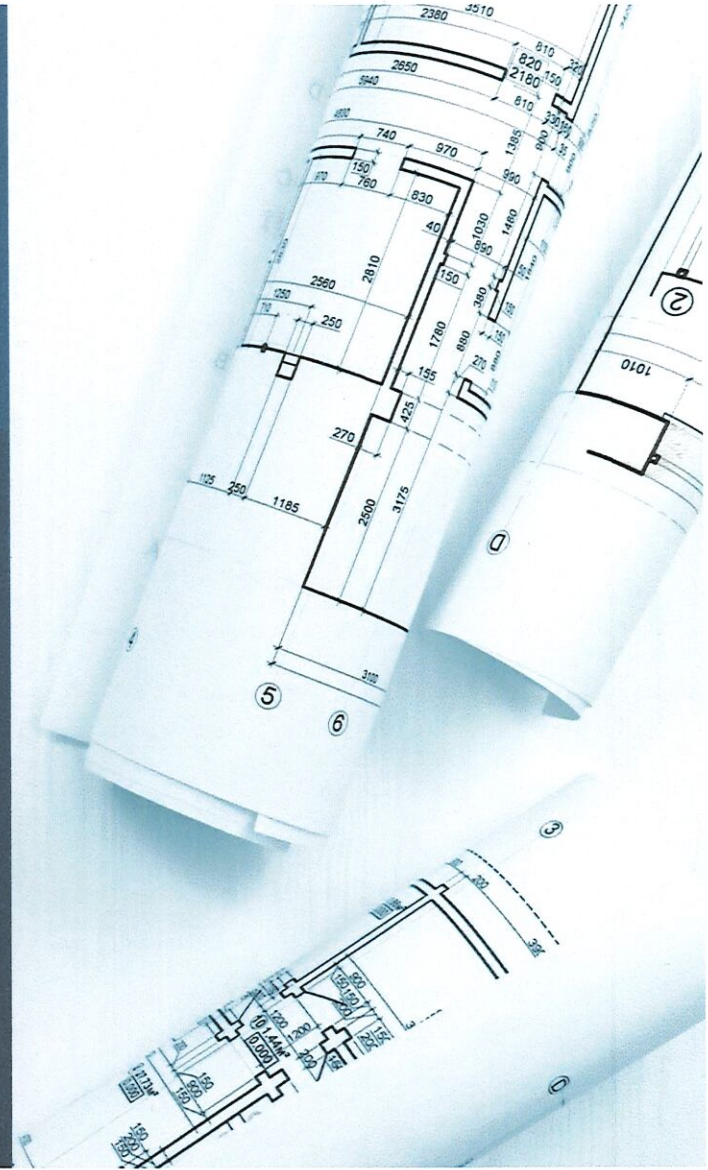
513-842-3021

mhuttlinger@cincyrealtoralliance.com

<https://cincyrealtoralliance.com/>



PROPOSAL FOR WAIVING BUILDING AND ZONING FEES



**BOARD OF COUNTY COMMISSIONERS
WARREN COUNTY, OHIO**

Resolution

Number 16-0120

Adopted Date January 26, 2016

ESTABLISH POLICY WITHIN THE WARREN COUNTY BUILDING AND ZONING DEPARTMENT RELATIVE TO THE WAIVING OF FEES FOR POLITICAL SUBDIVISIONS WITHIN WARREN COUNTY

WHEREAS, from time to time, this Board is requested to waive fees associated with a building, electrical and/or zoning permit from various political subdivision; and

WHEREAS, this Board desires to establish a policy relative to said fee waiver requests; and

NOW THEREFORE BE IT RESOLVED, to establish the following policy relative to the waiving of fees associated with political subdivisions within Warren County:

POLITICAL SUBDIVISION FEE WAIVER POLICY

1. Political subdivision shall submit a request for a waiver of building, electrical or zoning permits in writing to the Warren County Building and Zoning Department.
2. New construction, remodeling and/or building additions fewer than 5000 square feet shall have Warren County's portion of the fee waived at 100%.
3. New construction, remodeling or building additions over 5000 square feet shall have Warren County's portion of the fee waived at 50%.
4. All political subdivisions shall be responsible for the State of Ohio sur charge.

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

Mr. Young - yea
Mrs. South - yea
Mr. Grossmann - yea

Resolution adopted this 26th day of January 2016.

We request to add Non-Profits w
proof of 5013C.

Zoning Fees		Proposal	
Variance	\$750	Variance	\$400
Site Plan Review	\$500	Site Plan Review	\$400
Conditional Use	\$500	Conditional Use	\$400
Cost per case			
Board Members	\$250		
Legal Ad	\$65 - \$150		
Postage	\$40 - \$80		
Total *	\$355 - \$480		

*staff hours NOT included along with other items like paper, files, copies etc.

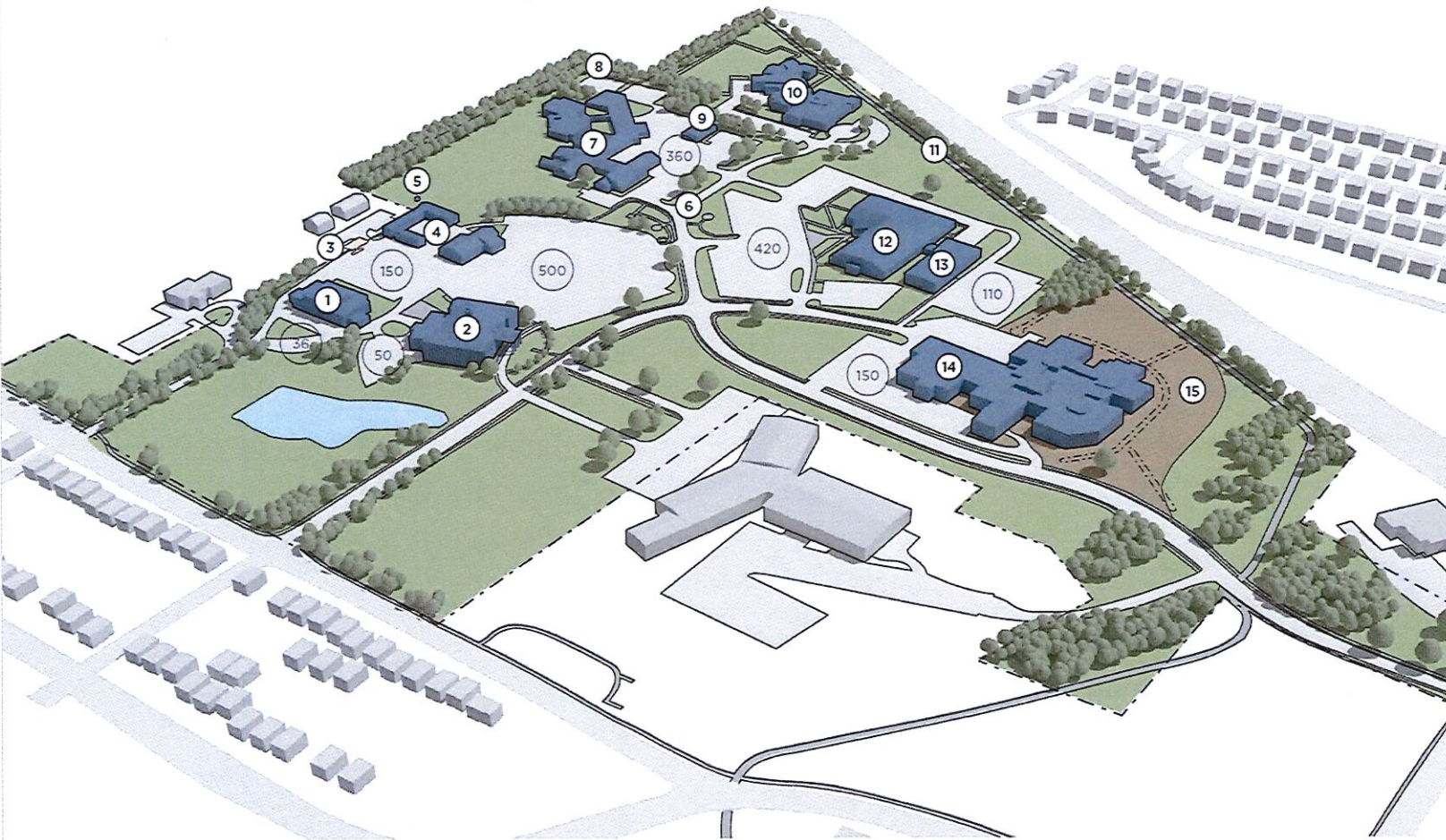
The image is a cover for a document titled "Warren County Master Plan". It features a photograph of the Warren County Courthouse, a large, classical-style building with a prominent dome. The building is set against a clear blue sky. In the foreground, there are trees with vibrant autumn foliage in shades of red, orange, and yellow. An American flag is visible on a tall pole to the left of the building. The title "Warren County Master Plan" is written in a white, elegant, italicized serif font, centered on a dark blue horizontal band that spans the width of the image.

*Warren County
Master Plan*

EXISTING

JUSTICE DRIVE CAMPUS

- ① Health & Human Services Building
 - ② Administration Building
 - ③ Fueling Station
 - ④ Facilities Management
 - ⑤ Weather Station
 - ⑥ Monuments
 - ⑦ County Court Building & Old Jail
 - ⑧ Impound Lot
 - ⑨ SWAT Garage
 - ⑩ Juvenile Justice Center
 - ⑪ Bike Trail
 - ⑫ Common Pleas Court Building (CPC)
 - ⑬ 520 Justice Office Building
 - ⑭ New Jail & Sheriff's Office
 - ⑮ Drainage
- # Parking Counts



PHASE
1A



DEMOLITION

- ① Demolish the existing Old Jail at 880 Memorial Drive. Note that the County Court Building is to remain and existing infrastructure that feeds County Court must be maintained.
- ② Construct a replacement SWAT garage and facility at an off-campus location. This 12,000 SF replacement facility will include SWAT vehicle storage, SWAT office and workspace, indoor and/or outdoor firearms training facilities, indoor large County vehicle storage, and secure indoor impounded vehicle storage. This step must be completed before the existing SWAT garage is demolished.
- ③ Demolish the existing SWAT garage.

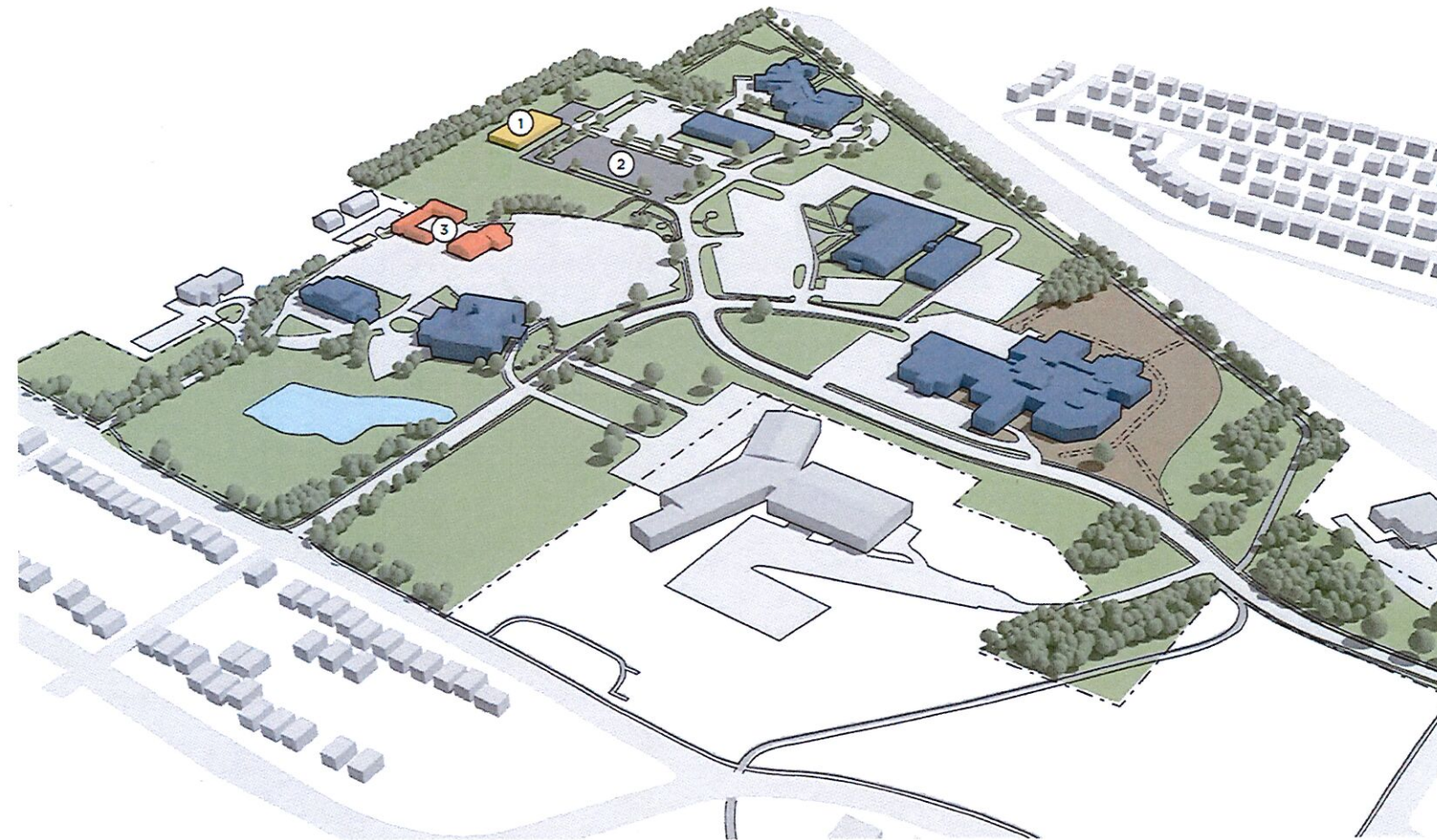
PHASE
1B



COUNTY COURT

- ① Construct a new County Court Building and adjacent parking lot.
- ② Demolish the existing County Court Building.

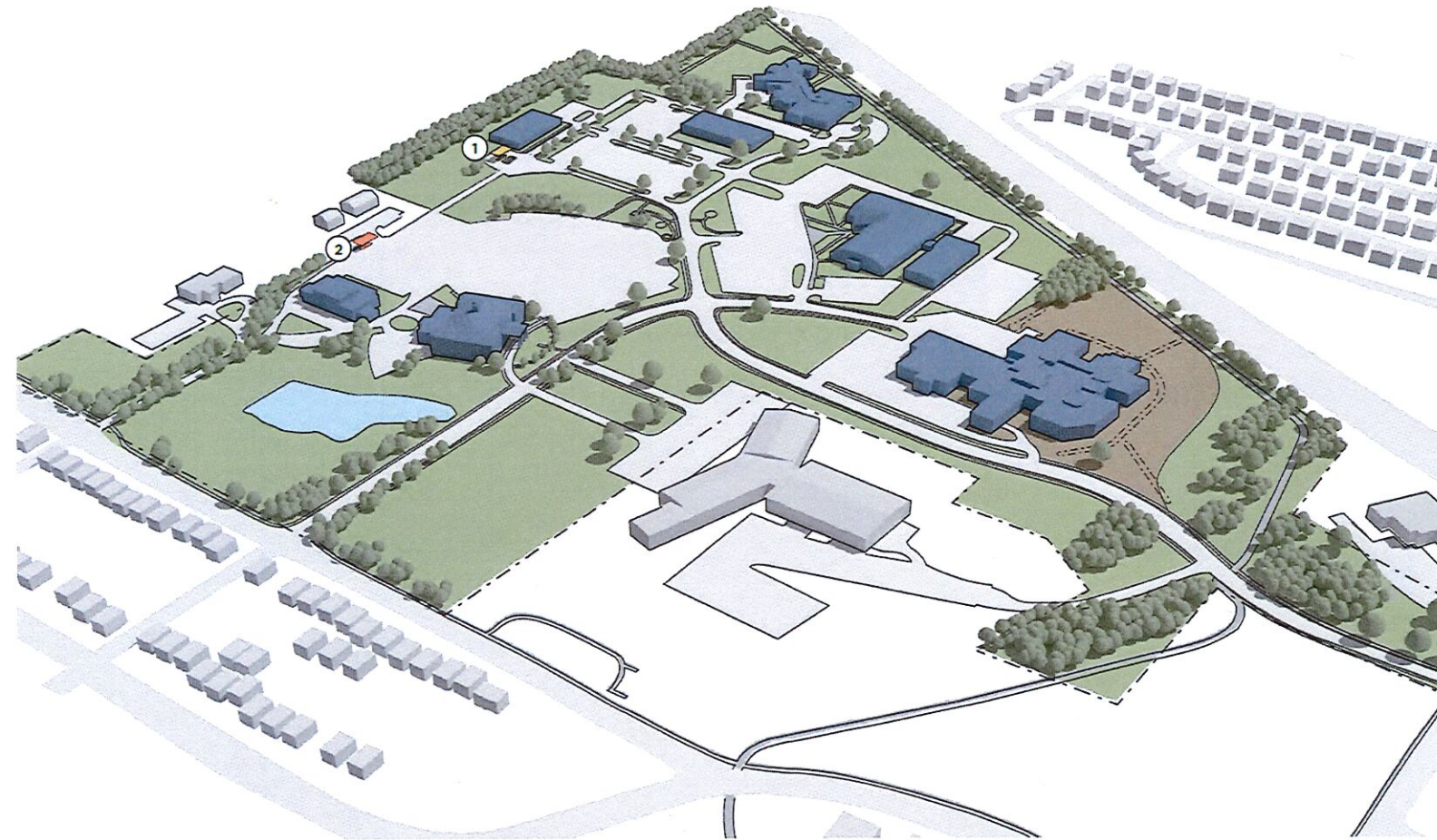
PHASE
1C



FACILITIES MANAGEMENT

- ① Construct a new 18,000 SF Facilities Management building. This step must be completed before the existing Facilities Management building is demolished.
- ② Create a new parking lot on the site of the demolished Old Jail and County Court Building.
- ③ Demolish existing Facilities Management building.

PHASE
1D



FUEL STATION

- ① Construct a new fueling station adjacent to the new Facilities Management building.
- ② Demolish existing fueling station.

END OF
PHASE 1



PLAN PHASE 2

- ① Demolition of Health & Human Services Building.
- ② Creates potential building sites for a new Health & Human Services building and new Board of Elections Building.

Phase 1

1. Demolish the old Jail and SWAT building
 - a. Leave County Court intact
 - b. Build a new tactical response and training facility off campus
2. Construct a new County Court facility, then demolish their current building
3. Construct a new Facilities Management building, then demolish their current building
4. Construct a new Fuel Station, then demolish the current station
5. Plan Phase 2 including a new Health & Human Services building and Board of Elections building.



**REQUEST FOR AUTHORIZATION TO ATTEND ASSOCIATION MEETING,
CONVENTION OR TRAINING SEMINAR/SESSION**

This form is to be completed by Department Head/Elected Official requesting authorization to attend an Association Meeting or Convention or Training Seminar/Session sponsored by an Association as required by O.R.C. Section 325.20. Additionally, authorization is required for any training seminar/session held more than 250 miles from county campus;

*NAME OF ATTENDEE: Jenny Carman DEPARTMENT: Children Services

*POSITION: Business Manager DATE: 4/24/23

REQUEST FOR AUTHORIZATION FOR THE ABOVE-NAMED EMPLOYEE/ELECTED OFFICIAL TO ATTEND THE FOLLOWING:

ASSOCIATION MEETING CONVENTION ASSOCIATION SPONSORED TRAINING SEMINAR/SESSION
TRAINING MORE THAN 250 MILES

PURPOSE:

CFIS Conference

LOCATION:

Nationwide Hotel and Conference Center, 100 Green Meadows Drive South,
Lewis Center, Ohio 43035

DATE(S): October 1-3, 2023

TYPE OF TRAVEL: (Check one)

AIRLINE STAFF CAR PRIVATE VEHICLE OTHER

LODGING: \$165/night x 3 x 1 night = \$495.00

ESTIMATED COST OF TRIP: Registration fee - TBD x 3 and meals \$20 x 3 = \$60.00

I CERTIFY THAT DIRECTION HAS BEEN GIVEN TO ALL EMPLOYEES ATTENDING THIS FUNCTION, THAT IT IS EXPECTED OF THEM TO ATTEND APPLICABLE SESSIONS.

DEPARTMENT HEAD/ELECTED OFFICIAL REQUESTING AUTHORIZATION:

Shawna Jones 4/24/23
Signature/Title Director Date

BOARD OF COMMISSIONERS' APPROVAL:

Commissioner Date

Commissioner Date

Commissioner Date

APR 25 '23 RCVD

RECEIVED OMB0000

*If additional employees will be attending the Association Meeting, Convention or Training Seminar/Session please list names and positions here:

Shawna Jones, Director and Katie Taylor, Assistant Business Manager



**REQUEST FOR AUTHORIZATION TO ATTEND ASSOCIATION MEETING,
CONVENTION OR TRAINING SEMINAR/SESSION**

This form is to be completed by Department Head/Elected Official requesting authorization to attend an Association Meeting or Convention or Training Seminar/Session sponsored by an Association as required by O.R.C. Section 325.20. Additionally, authorization is required for any training seminar/session held more than 250 miles from county campus;

*NAME OF ATTENDEE: Brandi Carter DEPARTMENT: Sheriff's Office

*POSITION: Detective DATE: 04/19/2023

REQUEST FOR AUTHORIZATION FOR THE ABOVE-NAMED EMPLOYEE/ELECTED OFFICIAL TO ATTEND THE FOLLOWING:

ASSOCIATION MEETING CONVENTION ASSOCIATION SPONSORED TRAINING
TRAINING MORE THAN 250 MILES SEMINAR/SESSION

PURPOSE:
Attend training related to her job duties.

LOCATION:
Atlanta, GA

DATE(S): 06/12/2023 - 06/15/2023

TYPE OF TRAVEL: (Check one)

AIRLINE STAFF CAR PRIVATE VEHICLE OTHER

LODGING: Hilton Inn

ESTIMATED COST OF TRIP: \$1000

I CERTIFY THAT DIRECTION HAS BEEN GIVEN TO ALL EMPLOYEES ATTENDING THIS FUNCTION, THAT IT IS EXPECTED OF THEM TO ATTEND APPLICABLE SESSIONS.

DEPARTMENT HEAD/ELECTED OFFICIAL REQUESTING AUTHORIZATION:

Larry D. Swift 4-20-2023
Signature/Title Date

BOARD OF COMMISSIONERS' APPROVAL:

Commissioner Date

Commissioner Date

Commissioner Date

RECEIVED OMB0000

*If additional employees will be attending the Association Meeting, Convention or Training Seminar/Session please list names and positions here:

APR 24 '23 ROWD



**REQUEST FOR AUTHORIZATION TO ATTEND ASSOCIATION MEETING,
CONVENTION OR TRAINING SEMINAR/SESSION**

This form is to be completed by Department Head/Elected Official requesting authorization to attend an Association Meeting or Convention or Training Seminar/Session sponsored by an Association as required by O.R.C. Section 325.20. Additionally, authorization is required for any training seminar/session held more than 250 miles from county campus;

*NAME OF ATTENDEE: Frances Ficke DEPARTMENT: Emergency Services

*POSITION: LEPC / Grants Coordinator DATE: 4/27/23

REQUEST FOR AUTHORIZATION FOR THE ABOVE-NAMED EMPLOYEE/ELECTED OFFICIAL TO ATTEND THE FOLLOWING:

ASSOCIATION MEETING CONVENTION ASSOCIATION SPONSORED TRAINING SEMINAR/SESSION
TRAINING MORE THAN 250 MILES

PURPOSE:
Emergency Management Fundamentals Course hosted by EMAO (Emergency Management Association of Ohio).

LOCATION:
12935 Stonecreek Drive, Pickerington OH 43147

DATE(S): June 2, 2023

TYPE OF TRAVEL: (Check one)
AIRLINE STAFF CAR PRIVATE VEHICLE OTHER

LODGING: N/A

ESTIMATED COST OF TRIP: \$50 (Course Fee)

I CERTIFY THAT DIRECTION HAS BEEN GIVEN TO ALL EMPLOYEES ATTENDING THIS FUNCTION, THAT IT IS EXPECTED OF THEM TO ATTEND APPLICABLE SESSIONS.

DEPARTMENT HEAD/ELECTED OFFICIAL REQUESTING AUTHORIZATION:
Melina Rowe 4-27-23
Signature/Title Date

BOARD OF COMMISSIONERS' APPROVAL:

Commissioner Date

Commissioner Date

Commissioner Date

*If additional employees will be attending the Association Meeting, Convention or Training Seminar/Session please list names and positions here:

APR 27
RECEIVED OMB0000



**REQUEST FOR AUTHORIZATION TO ATTEND ASSOCIATION MEETING,
CONVENTION OR TRAINING SEMINAR/SESSION**

This form is to be completed by Department Head/Elected Official requesting authorization to attend an Association Meeting or Convention or Training Seminar/Session sponsored by an Association as required by O.R.C. Section 325.20. Additionally, authorization is required for any training seminar/session held more than 250 miles from county campus;

*NAME OF ATTENDEE: Shawna Jones DEPARTMENT: Children Services

*POSITION: Director DATE: 4/25/2023

REQUEST FOR AUTHORIZATION FOR THE ABOVE-NAMED EMPLOYEE/ELECTED OFFICIAL TO ATTEND THE FOLLOWING:

ASSOCIATION MEETING CONVENTION ASSOCIATION SPONSORED TRAINING SEMINAR/SESSION
TRAINING MORE THAN 250 MILES

PURPOSE: NaCo Annual Conference

LOCATION: Travis County Texas

DATE(S): 7/21/23-7/24/23

TYPE OF TRAVEL: (Check one)

AIRLINE STAFF CAR PRIVATE VEHICLE OTHER

LODGING: Hotel to be determined

ESTIMATED COST OF TRIP: \$1850 (\$600 registration fee; Hotel \$250 x 5 night)

I CERTIFY THAT DIRECTION HAS BEEN GIVEN TO ALL EMPLOYEES ATTENDING THIS FUNCTION, THAT IT IS EXPECTED OF THEM TO ATTEND APPLICABLE SESSIONS.

DEPARTMENT HEAD/ELECTED OFFICIAL REQUESTING AUTHORIZATION:

Shawna Jones 4-26-23
Signature/Title Date

BOARD OF COMMISSIONERS' APPROVAL:

Commissioner Date

Commissioner Date

Commissioner Date

*If additional employees will be attending the Association Meeting, Convention or Training Seminar/Session please list names and positions here:

Osborne, Tina

From: Wright, Barney
Sent: Wednesday, April 12, 2023 12:49 PM
To: Jim McCourt; Spaeth, James L.; Nolan, Matthew; rskuvn@gmail.com; Osborne, Tina
Cc: Swigert, David L.
Subject: 1st Quarter IAC report
Attachments: 3-23 IAC Report.xlsx

Good Afternoon,

I have attached the TOS report for March, with added calculations for Weighted Average Yield and Weighted Maturity for the Portfolio.

Looking back at February, there is a slight lengthening of the portfolio maturity and a slight decrease in the yield. I believe both of these can be attributed to the \$27,000,000 decrease in our STAR balance – funds distributed to the various entities for which we collect tax. We will see something over \$70,000,000 additionally distributed for final settlement this week, so I anticipate similar changes in our yield and maturity will happen in April.

Our STAR balance has produced a real windfall in interest earnings for us this year. We earned \$1,183.04 in January, \$263,492.78 in February and \$453,265.86 in March. Given the highly inverted yield curve we will do well to keep a slightly larger “reserve fund” at STAR than we might otherwise.

Please feel free to pass on any questions I might answer.

Barney Wright

Treasurer, Warren County
406 Justice Dr.
Lebanon, OH 45036

513.695.1300

Barney.wright@co.warren.oh.us

Warren County Investment Portfolio
3/31/2023

CUSIP Id	Asset Short Name	Maturity Date	Shares/Par	Federal Tax Cost Amt	Yield	WAY	Days to Maturity	Weighted Maturity
	STAR OH	4/1/2023	102,780,048.0000	102,780,048.00	5.020000000	1.125080443	1	0.22411961
31846V567	FIRST AM GOVT OB FD CL Z	4/1/2023	318,304.5700	318,304.57	4.626448000	0.003211157	1	0.000694087
89236TJD8	TOYOTA MOTOR MTN 0.400% 4/06/23	04/06/2023	2,000,000.0000	2,001,780.00	0.400000000	0.001746013	6	0.026190189
12738RGA6	CADENCE BK N A C D 1.300% 4/17/23	04/17/2023	248,000.0000	247,380.00	1.300754438	0.000701667	17	0.009170321
33847E3B1	FLAGSTAR BK FSB C D 1.150% 5/01/23	05/01/2023	248,000.0000	247,442.00	1.152327702	0.000621757	31	0.016726542
48133DE71	JPMORGAN LLC MTN 2.500% 5/01/23	05/01/2023	3,000,000.0000	3,000,000.00	2.505487017	0.016390208	31	0.202793481
22533US95	CREDIT AGRICOLE C P 5/09/23	05/09/2023	3,000,000.0000	2,918,100.00	3.740000000	0.023798129	39	0.248162308
023135BV7	AMAZON COM INC 0.250% 5/12/23	05/12/2023	2,000,000.0000	2,001,300.00	0.250868003	0.001094784	42	0.183287365
63873KSF5	NATIXIS N Y BRH DISC C P 5/15/23	05/15/2023	3,000,000.0000	2,917,096.67	3.850000000	0.024489651	45	0.286242672
46640QT68	J P MORGAN SECS C P 6/06/23	06/06/2023	4,690,000.0000	4,554,341.75	4.020000000	0.039922958	67	0.665382633
69353RFL7	PNC BANK NA MTN 3.500% 6/08/23	06/08/2023	2,388,000.0000	2,415,175.44	3.514020944	0.018506491	69	0.363386523
13607FU79	CANADIAN IMPERIAL C P 7/07/23	07/07/2023	3,718,000.0000	3,587,911.31	4.870000000	0.038101467	98	0.766723575
	1st NATIONAL BANK 0.5% 7/20/23	07/20/2023	1,000,000.0000	1,000,000.00	0.500000000	0.001090288	111	0.242043832
8923A1UM1	TOYOTA CR DE PUERTO CORP C P 7/21/23	07/21/2023	2,500,000.0000	2,404,881.25	5.330000000	0.027950648	112	0.587330699
17330PNQ8	CITIGROUP GLOBAL MTN 3.800% 7/30/23	07/30/2023	2,000,000.0000	2,000,000.00	3.815031223	0.016637924	121	0.527699166
	1st NATIONAL BANK 3.25% 8/22/23	08/22/2023	2,000,000.0000	2,000,000.00	3.250000000	0.014173738	144	0.628005619
75472RAD3	RAYMOND JAMES C D 1.950% 8/23/23	08/23/2023	247,000.0000	246,506.00	1.971150444	0.001059542	145	0.077941101
3137EAEV7	F H L M C M T N 0.250% 8/24/23	08/24/2023	2,500,000.0000	2,497,450.00	0.254419263	0.001385536	146	0.795098072
62479MVR1	MUFG BANK LTD C P 8/25/23	08/25/2023	3,000,000.0000	2,884,983.33	5.360000000	0.033719346	147	0.924765664
62479MW82	MUFG BK LTD N Y BRH C P 9/08/23	09/08/2023	4,500,000.0000	4,327,537.50	5.310000000	0.050107923	161	1.519279781
14913R2F3	CATERPILLAR FINL MTN 0.450% 9/14/23	09/14/2023	1,680,000.0000	1,676,606.40	0.458295142	0.001675512	167	0.610546341
31422BG53	F A M C M T N 0.350% 9/29/23	09/29/2023	3,000,000.0000	2,997,600.00	0.357398142	0.00233613	182	1.189641512
46513JCT6	ISRAEL ST 1.160% 10/01/23	10/01/2023	1,500,000.0000	1,500,000.00	1.176936111	0.003849596	184	0.601838719
3137EAEY1	F H L M C M T N 0.125% 10/16/23	10/16/2023	2,000,000.0000	1,992,540.00	0.128115776	0.000556648	199	0.864631726
3133EK3M6	F F C B DEB 1.625% 10/23/23	10/23/2023	2,000,000.0000	1,998,080.00	1.653523277	0.00720434	206	0.897534467
8923A1XT3	TOYOTA CDT DE PR CORP C P 10/27/23	10/27/2023	2,000,000.0000	1,923,650.00	5.290000000	0.022189768	210	0.880879278
3134GW6E1	F H L M C M T N 0.320% 11/02/23	11/02/2023	2,000,000.0000	2,000,000.00	0.328383634	0.00143213	216	0.942008429
	1ST NATIONAL BANK 4.8% 11/9/23	11/09/2023	2,000,000.0000	2,000,000.00	4.800000000	0.020933521	223	0.97253648
3134GXAY0	F H L M C M T N 0.300% 11/13/23	11/13/2023	2,000,000.0000	1,998,500.00	0.308626099	0.001344955	227	0.989238595
239876CR4	DAYTON OH SPL 0.631% 12/01/23	12/01/2023	875,000.0000	875,000.00	0.648876549	0.001238059	245	0.46746078
935165AG5	WARREN CNTY OH 3.750% 12/01/23	12/01/2023	175,000.0000	175,000.00	3.817493281	0.001456758	245	0.093492156
9AMBDF8K2	WARREN CNTY VPSA R19 4.650% 12/01/23	12/01/2023	14,757.0000	14,757.00	4.650000000	0.000149631	245	0.007883793
9AMBDF913	WCPA TIF RACINO 3.200% 12/01/23	12/01/2023	390,000.0000	390,000.00	3.200000000	0.002721358	245	0.208353948
06406RAP2	BANK NEW YORK MTN 0.350% 12/07/23	12/07/2023	2,000,000.0000	2,000,000.00	0.362236344	0.001579767	251	1.094648684
3130AU6T6	F H L B DEB 4.750% 12/12/23	12/12/2023	2,750,000.0000	2,746,617.50	4.751995838	0.02846068	256	1.533236644
89236THU2	TOYOTA MOTOR MTN 0.450% 1/11/24	01/11/2024	1,000,000.0000	1,002,200.00	0.465539716	0.001017378	286	0.625016487
3133EMNG3	F F C B DEB 0.230 1/19/24	01/19/2024	1,575,000.0000	1,572,905.25	0.238334560	0.000817449	294	1.008372364
91282CBM2	U S TREASURY NT 0.125% 2/15/24	02/15/2024	3,500,000.0000	3,483,730.47	0.129917373	0.000986922	321	2.438487993
3134GWXC5	F H L M C 0.350% 3/29/24	03/29/2024	2,500,000.0000	2,498,750.00	0.365313961	0.001990491	364	1.98333115
91282CEG2	U S TREASURY NT 2.250% 3/31/24	03/31/2024	3,975,000.0000	3,915,375.00	2.302237775	0.019655975	366	3.124823492
3133EMWV0	F F C B DEB 0.350% 4/22/24	04/22/2024	1,000,000.0000	1,000,000.00	0.365111985	0.000796154	388	0.846063126
91282CEK3	U S TREASURY NT 2.500% 4/30/24	04/30/2024	4,000,000.0000	3,954,687.50	2.555819089	0.022040088	396	3.414903213
023135BW5	AMAZON COM INC 0.450% 5/12/24	05/12/2024	2,000,000.0000	1,999,220.00	0.471041420	0.002053481	408	1.778655309
3130ANM49	F H L B DEB 0.400% 5/24/24	05/24/2024	3,000,000.0000	2,999,100.00	0.419630306	0.002744283	420	2.746700328
3133EKQU3	F F C B DEB 1.950% 6/13/24	06/13/2024	1,500,000.0000	1,498,290.00	2.010682395	0.006569168	440	1.43753888
3130A8HK2	F H L B DEB 1.750% 6/14/24	06/14/2024	850,000.0000	847,977.00	1.810544612	0.003347837	441	0.815443179
91282CCG4	U S TREASURY NT 0.250% 6/15/24	06/15/2024	6,695,000.0000	6,654,043.56	0.262756845	0.003812508	442	6.413261537

89236TJH9	TOYOTA MTR CR MTN	0.500%	6/18/24	06/18/2024	4,409,000.0000	4,391,364.00	0.524901319	0.005026297	445	4.261185989
3133ENZS2	F F C B DEB	3.100%	6/28/24	06/28/2024	4,000,000.0000	3,998,560.00	3.155762320	0.027515597	455	3.96721791
3135G0V75	F N M A	1.750%	7/02/24	07/02/2024	5,000,000.0000	4,992,495.00	1.812532367	0.019732152	459	4.996908146
3130AN6Y1	F H L B DEB	0.500%	7/26/24	07/26/2024	2,500,000.0000	2,500,000.00	0.527042553	0.00287314	483	2.633044394
3133EKVV4	F F C B DEB	1.850%	7/26/24	07/26/2024	1,250,000.0000	1,248,225.00	1.920421870	0.005227097	483	1.314652736
3130ANB33	F H L B DEB	0.500%	7/29/24	07/29/2024	1,500,000.0000	1,500,000.00	0.527181477	0.001724338	486	1.589639224
15118RRH2	CELTIC BANK C D	1.82466%	8/30/24	08/30/2024	249,000.0000	248,285.37	1.904293974	0.001030994	518	0.280447732
3133EL5S9	F F C B DEB	0.480%	9/03/24	09/03/2024	4,250,000.0000	4,248,725.00	0.507737711	0.004704019	522	4.836154506
91282CCX7	U S TREASURY NT	0.375%	9/15/24	09/15/2024	2,750,000.0000	2,744,628.91	0.396695264	0.002374169	534	3.195920244
3133EKP75	F F C B	1.600%	9/17/24	09/17/2024	2,000,000.0000	1,996,000.00	1.663270822	0.007239266	536	2.332901319
3133ELEA8	F F C B DEB	1.700%	9/17/24	09/17/2024	2,500,000.0000	2,497,300.00	1.764766947	0.009610127	536	2.918814862
3133EMBD3	F F C B DEB	0.360%	9/24/24	09/24/2024	1,500,000.0000	1,498,125.00	0.384648261	0.001256559	543	1.773858295
3134GWUS3	F H L M C M T N	0.400%	9/24/24	09/24/2024	3,500,000.0000	3,499,825.00	0.427135947	0.003259744	543	4.143975707
912828YH7	U S TREASURY NT	1.500%	9/30/24	09/30/2024	3,000,000.0000	2,971,875.00	1.562434899	0.010125198	549	3.557737694
3135G0W66	F N M A	1.625%	10/15/24	10/15/2024	5,500,000.0000	5,490,355.00	1.688399397	0.020213739	564	6.752282011
3133EK3B0	F F C B DEB	1.500%	10/16/24	10/16/2024	6,000,000.0000	5,989,788.54	1.564308732	0.020431723	565	7.379568706
06406RAX5	BANK NEW YORK MTN	0.850%	10/25/24	10/25/2024	3,345,000.0000	3,340,379.40	0.910103216	0.006629145	574	4.180986173
172254VWM2	CINCINNATI OHIO	0.879%	11/01/24	11/01/2024	390,000.0000	390,000.00	0.933785176	0.000794114	581	0.494096505
3133EK4Y9	F F C B DEB	1.650%	11/01/24	11/01/2024	3,000,000.0000	2,983,560.00	1.718499386	0.011180345	581	3.779914275
3133EK6J0	F F C B DEB	1.625%	11/08/24	11/08/2024	2,500,000.0000	2,498,075.00	1.699239786	0.009256167	588	3.202977156
3134GWL1	F H L M C M T N	0.500%	11/27/24	11/27/2024	2,500,000.0000	2,500,000.00	0.536503713	0.002924717	607	3.309022665
856285RS2	STATE BANK OF C D	2.050%	11/27/24	11/27/2024	247,000.0000	246,135.50	2.145945210	0.001151765	607	0.325787179
232285BM7	CUYAHOGA CNTY OH	0.589%	12/01/24	12/01/2024	1,565,000.0000	1,565,000.00	0.630115004	0.00215033	611	2.085098588
531677PD8	LICKING HEIGHTS OH	0.880%	12/01/24	12/01/2024	350,000.0000	350,000.00	0.934817711	0.000713454	611	0.466315978
935165AH3	WARREN CNTY OH PORT	3.880%	12/01/24	12/01/2024	180,000.0000	180,000.00	4.018976197	0.001577462	611	0.239819646
9AMBDF8L0	WARREN CNTY VPSA R20	4.750%	12/01/24	12/01/2024	15,444.0000	15,444.00	4.750000000	0.000159965	611	0.020576526
677581JB7	OHIO ST	0.520%	12/15/24	12/15/2024	1,230,000.0000	1,230,000.00	0.556602158	0.001492867	625	1.676317083
3134GV7E2	F H L M C M T N	0.500%	1/27/25	01/27/2025	2,000,000.0000	1,994,400.00	0.540447058	0.002350371	668	2.905091195
3133EMSJ2	F F C B DEB	0.430%	3/03/25	03/03/2025	6,250,000.0000	6,222,600.00	0.461239770	0.006258492	703	9.53889903
912828ZF0	U S TREASURY NT	0.500%	3/31/25	03/31/2025	4,000,000.0000	3,986,718.75	0.535544059	0.004655666	731	6.35483118
3133EMUP5	F F C B DEB	0.710%	4/01/25	04/01/2025	3,000,000.0000	3,000,000.00	0.760309692	0.004973737	732	4.788542848
3130AN7M6	F H L B DEB	0.625%	4/21/25	04/21/2025	3,000,000.0000	2,998,500.00	0.671414913	0.004390016	752	4.916917664
3135G03U5	F N M A DEB	0.625%	4/22/25	04/22/2025	5,000,000.0000	4,991,250.00	0.670550495	0.007298134	753	8.195497865
3130ANAY6	F H L B DEB	0.700%	4/29/25	04/29/2025	1,830,000.0000	1,830,000.00	0.751306737	0.002998054	760	3.032743804
3133EMYN6	F F C B DEB	0.710%	5/06/25	05/06/2025	1,620,000.0000	1,620,000.00	0.762162394	0.002692363	767	2.709451744
3133ELC28	F F C B DEB	0.730%	5/27/25	05/27/2025	2,000,000.0000	1,997,500.00	0.784541312	0.003417226	788	3.432290574
3133ELH23	F F C B DEB	0.500%	6/09/25	06/09/2025	3,000,000.0000	2,994,690.00	0.539432517	0.003522573	801	5.230647226
7954506N0	SALLIE MAE BANK C D	0.800%	6/10/25	06/10/2025	249,000.0000	247,755.00	0.872429061	0.000471328	802	0.433279197
88241THU7	TEXAS EXCHANGE C	0.92055%	6/19/25	06/19/2025	249,000.0000	248,004.00	1.001095765	0.000541384	811	0.438581776
3133EMU34	F F C B DEB	0.680%	7/21/25	07/21/2025	1,250,000.0000	1,250,000.00	0.733921190	0.002000463	843	2.297780977
911759KU1	U S DEPT HSG & URB	4.130%	8/01/25	08/01/2025	370,000.0000	372,489.73	4.129256734	0.003353955	854	0.693654513
3136G4H71	F N M A	0.500%	8/18/25	08/18/2025	1,000,000.0000	993,390.00	0.543206658	0.001176673	871	1.886726637
3136G4J53	F N M A	0.600%	8/18/25	08/18/2025	2,000,000.0000	1,995,100.00	0.650173922	0.002828559	871	3.789255291
3136G4J95	F N M A	0.550%	8/25/25	08/25/2025	2,000,000.0000	1,997,500.00	0.602290896	0.002623398	878	3.824303456
3136G4W41	F N M A	0.650%	8/25/25	08/25/2025	2,500,000.0000	2,501,175.00	0.703851693	0.003838807	878	4.788611864
3136G4X40	F N M A M T N	0.600%	8/26/25	08/26/2025	1,585,000.0000	1,585,000.00	0.650540491	0.002248406	879	3.038009893
3136G4H89	F N M A	0.600%	8/27/25	08/27/2025	1,000,000.0000	996,420.00	0.650582814	0.001413566	880	1.912036376
3137EAEX3	F H L M C M T N	0.375%	9/23/25	09/23/2025	5,000,000.0000	4,924,900.00	0.409540659	0.004398104	907	9.740376534
46513JET4	ISRAEL ST	1.420%	10/01/25	10/01/2025	2,000,000.0000	2,000,000.00	1.526372929	0.006656742	915	3.990452374
3134GWZV1	F H L M C M T N	0.650%	10/22/25	10/22/2025	590,000.0000	581,740.00	0.715496555	0.000907627	936	1.187341964
3134GW5P7	F H L M C M T N	0.600%	10/27/25	10/27/2025	1,500,000.0000	1,499,325.00	0.661587148	0.002162987	941	3.076496661
3136G45C3	F N M A	0.540%	10/27/25	10/27/2025	2,000,000.0000	1,998,000.00	0.589217323	0.002567096	941	4.099738435

3134GW4B9	F H L M C M T N	0.500%	10/29/25	10/29/2025	2,500,000.0000	2,495,000.00	0.550788178	0.002996582	943	5.13042431
3135G06G3	F N M A	0.500%	11/07/25	11/07/2025	4,750,000.0000	4,476,147.50	0.546155611	0.005330793	952	9.292068007
935165AJ9	WARREN CNTY OH PORT	3.980%	12/01/25	12/01/2025	190,000.0000	190,000.00	4.170552546	0.001727899	976	0.404365841
9AMBDF8M8	WARREN CNTY UTICA RD	4.400%	12/01/25	12/01/2025	13,891.0000	13,891.00	4.400000000	0.000133278	976	0.029563399
9AMBDF8N6	WARREN CNTY SHAKER	4.400%	12/01/25	12/01/2025	1,133.0000	1,133.00	4.400000000	1.08706E-05	976	0.002411297
9AMBDJN01	WARREN COUNTY, OHIO	2.200%	12/01/25	12/01/2025	987,000.0000	987,000.00	2.200000000	0.004734901	976	2.100574129
3134GXFV1	F H L M C M T N	0.625%	12/17/25	12/17/2025	3,000,000.0000	2,998,500.00	0.684376506	0.004474765	992	6.486146705
3134GXGZ1	F H L M C M T N	0.550%	12/30/25	12/30/2025	1,000,000.0000	1,000,000.00	0.601987654	0.001312679	1005	2.191477943
3135G06Q1	F N M A	0.640%	12/30/25	12/30/2025	2,000,000.0000	2,002,600.00	0.701200806	0.003062017	1005	4.388653728
91282CBC4	U S TREASURY NT	0.375%	12/31/25	12/31/2025	2,200,000.0000	2,136,664.06	0.410958904	0.001914722	1006	4.687111315
31422B6K1	F A M C M T N	0.480%	1/15/26	01/15/2026	1,500,000.0000	1,498,500.00	0.526506302	0.001720408	1021	3.336211165
3130AKQM1	F H L B DEB	0.700%	1/27/26	01/27/2026	7,200,000.0000	7,118,568.00	0.767291461	0.011910337	1033	16.03481677
3135G06R9	F N M A	0.550%	1/28/26	01/28/2026	2,500,000.0000	2,500,000.00	0.605813608	0.003302555	1034	5.63678655
3130AKV37	F H L B DEB	0.530%	2/04/26	02/04/2026	3,205,000.0000	3,169,745.00	0.584846947	0.004042384	1041	7.195253461
3130AKXB7	F H L B DEB	0.580%	2/11/26	02/11/2026	2,000,000.0000	1,992,000.00	0.639456682	0.002777612	1048	4.5522034
199098DK7	COLUMBUS FRANKLIN OH	1.501%	2/15/26	02/15/2026	1,035,000.0000	1,067,726.70	1.651773924	0.003845756	1052	2.449327648
3133EMQX3	F F C B DEB	0.590%	2/17/26	02/17/2026	2,500,000.0000	2,490,225.00	0.650582216	0.003532741	1054	5.723349165
3130AKVV5	F H L B DEB	0.500%	2/18/26	02/18/2026	3,000,000.0000	3,000,000.00	0.552828269	0.003616451	1055	6.901520089
3130AL6C3	F H L B DEB	0.400%	2/18/26	02/18/2026	1,000,000.0000	980,000.00	0.438418624	0.000936885	1055	2.254496562
3133EMUK6	F F C B DEB	1.050%	3/25/26	03/25/2026	2,750,000.0000	2,750,000.00	1.146050492	0.006872385	1090	6.536273765
91282CCJ8	U S TREASURY NT	0.875%	6/30/26	06/30/2026	4,500,000.0000	4,487,167.97	0.957791497	0.009371613	1187	11.61432803
3130AN3Y4	F H L B DEB	1.100%	7/13/26	07/13/2026	5,000,000.0000	5,000,000.00	1.206444608	0.013153715	1200	13.08345041
3130ANAD2	F H L B DEB	1.000%	7/29/26	07/29/2026	3,750,000.0000	3,750,000.00	1.101624897	0.009008159	1216	9.943422308
91282CCP4	U S TREASURY NT	0.625%	7/31/26	07/31/2026	3,500,000.0000	3,450,234.38	0.691501720	0.00520251	1218	9.163616991
3130ANMH0	F H L B DEB	1.100%	8/20/26	08/20/2026	2,410,000.0000	2,230,310.40	1.209801593	0.0058837	1238	6.020838753
91282CCW9	U S TREASURY NT	0.750%	8/31/26	08/31/2026	2,830,000.0000	2,817,176.56	0.828372304	0.005088745	1249	7.672688145
3133EM6E7	F F C B DEB	0.940%	9/28/26	09/28/2026	2,150,000.0000	2,143,550.00	1.042660337	0.004873573	1277	5.968917243
3130AP3E3	F H L B DEB	0.820%	9/30/26	09/30/2026	1,200,000.0000	1,192,800.00	0.916487840	0.002383776	1279	3.326666134
91282CCZ2	U S TREASURY NT	0.875%	9/30/26	09/30/2026	3,500,000.0000	3,478,535.16	0.963773144	0.007310419	1279	9.701479806
3130APB87	F H L B DEB	1.100%	10/13/26	10/13/2026	3,250,000.0000	3,244,800.00	1.214463152	0.00859297	1292	9.141584733
91282CDK4	U S TREASURY NT	1.250%	11/30/26	11/30/2026	1,850,000.0000	1,853,685.53	1.363438045	0.005511154	1340	5.416414603
172311RM6	CINCINNATI OH	1.200%	12/01/26	12/01/2026	545,000.0000	545,000.00	1.335916104	0.001587621	1341	1.593662385
935165AK6	WARREN CNTY OH	4.080%	12/01/26	12/01/2026	200,000.0000	200,000.00	4.311893640	0.001880482	1341	0.584830233
172253FN1	CINCINNATI OH CITY	1.471%	12/15/26	12/15/2026	1,490,000.0000	1,490,000.00	1.636298917	0.005316428	1355	4.402472033
3130ALED2	F H L B DEB	1.020%	2/24/27	02/24/2027	4,000,000.0000	3,593,040.00	1.137719876	0.008913914	1426	11.17255805
3130ALCE2	F H L B DEB	0.920%	2/26/27	02/26/2027	3,000,000.0000	2,697,210.00	1.030258236	0.006059432	1428	8.398737558
91282CEF4	U S TREASURY NT	2.500%	3/31/27	03/31/2027	1,350,000.0000	1,308,076.17	2.611593385	0.0074492	1461	4.167295451
91282CEN7	U S TREASURY NT	2.750%	4/30/27	04/30/2027	3,000,000.0000	2,998,007.81	2.847321447	0.018614025	1491	9.747235194
91282CET4	U S TREASURY NT	2.625%	5/31/27	05/31/2027	3,000,000.0000	2,983,828.13	2.731813924	0.017774441	1522	9.902833986
91282CEW7	U S TREASURY NT	3.250%	6/30/27	06/30/2027	4,750,000.0000	4,746,289.06	3.300263006	0.034156533	1552	16.06264064
91282CFB2	U S TREASURY NT	2.750%	7/31/27	07/31/2027	2,300,000.0000	2,173,589.84	2.848707723	0.013501951	1583	7.502906811
3133ENG87	F F C B DEB	2.920%	8/17/27	08/17/2027	2,870,000.0000	2,849,135.10	3.031687362	0.018835125	1600	9.940404741
91282CFH9	U S TREASURY NT	3.125%	8/31/27	08/31/2027	2,500,000.0000	2,447,753.91	3.187116909	0.017011272	1614	8.614742992
91282CFM8	U S TREASURY NT	4.125%	9/30/27	09/30/2027	3,250,000.0000	3,272,978.52	4.040077569	0.028833934	1644	11.73318749
3133ENW63	F F C B DEB	4.375%	10/27/27	10/27/2027	2,800,000.0000	2,806,055.28	4.280989471	0.026194579	1671	10.2245385
91282CFZ9	U S TREASURY NT	3.875%	11/30/27	11/30/2027	4,500,000.0000	4,473,281.25	3.825837982	0.037318469	1705	16.63112509
935165AL4	WARREN CNTY OH	4.210%	12/01/27	12/01/2027	205,000.0000	205,000.00	4.445007549	0.001986998	1706	0.762612518
9AMBDFML4	WARREN CO SPEC OB RV	2.570%	12/01/27	12/01/2027	560,000.0000	560,000.00	2.570000000	0.003138284	1706	2.083234197
3130ATUS4	F H L B DEB	4.250%	12/10/27	12/10/2027	3,300,000.0000	3,368,376.00	4.172885084	0.030649827	1715	12.59666938
91282CGH8	U S TREASURY NT	3.500%	1/31/28	01/31/2028	4,500,000.0000	4,341,445.32	3.509334831	0.033222337	1767	16.72791939
91282CGP0	U S TREASURY NT	4.000%	2/29/28	02/29/2028	4,500,000.0000	4,443,750.00	3.919455196	0.037979248	1796	17.4031151
3133EPCX1	F F C B DEB	4.375%	3/10/28	03/10/2028	2,250,000.0000	2,245,995.00	4.267376758	0.020899737	1806	8.844994622

199492R92	COLUMBUS OH	1.215%	4/01/28	04/01/2028	500,000.0000	500,000.00	1.403764168	0.001530507	1828	1.993045612
9141193T7	UNIVERSITY OH	1.598%	6/01/28	06/01/2028	1,000,000.0000	1,000,000.00	1.824159266	0.003977716	1889	4.119106303
935165AM2	WARREN CNTY OH	4.310%	12/01/28	12/01/2028	215,000.0000	215,000.00	4.540330991	0.002128614	2072	0.971402581
9AMBDFMK6	WARREN CO SPEC OB RV	2.570%	12/01/28	12/01/2028	1,295,000.0000	1,295,000.00	2.570000000	0.007257281	2072	5.851006244
935163AX3	WARREN CNTY OH PORT	2.390%	12/01/29	12/01/2029	1,535,000.0000	1,535,000.00	2.390000000	0.007999767	2437	8.15708431
9AMBDFNN9	WCPA MIDDLETOWN PACE	3.090%	12/01/29	12/01/2029	295,000.0000	295,000.00	3.090000000	0.001987703	2437	1.567648125
9AMBDK342	WARREN COUNTY BLP	3.030%	6/01/31	06/01/2031	684,000.0000	684,000.00	3.030000000	0.004519285	2984	4.450675825
9AMBDF8Q9	WARREN CNTY BELLBROO	4.500%	12/01/33	12/01/2033	203,913.0000	203,913.00	4.500000000	0.002000914	3898	1.733236359
9AMBDF8Z9	WARREN COUNTY	6.500%	12/01/35	12/01/2035	1,650,000.0000	1,650,000.00	6.500000000	0.023386668	4628	16.65130733
9AMBDF8T3	WARREN CNTY OLD 122	4.000%	12/01/36	12/01/2036	276,575.0000	276,575.00	4.000000000	0.00241237	4994	3.011844191
9AMBDF8W6	WARREN COUNTY	4.625%	12/01/36	12/01/2036	16,022.0000	16,022.00	4.625000000	0.000161584	4994	0.174476246
9AMBDF8U0	WARREN CNTY IRWIN-SI	4.210%	12/01/37	12/01/2037	106,870.1800	106,870.18	4.210000000	0.000981092	5359	1.248853053
9AMBDFZ71	COUNTY OF WARREN	2.300%	12/01/39	12/01/2039	547,000.0000	547,000.00	2.300000000	0.002743381	6089	7.262804308
					461,806,957.7500	458,594,622.5300	312.2027	2.4399		650.9750 Days
										1.783493155 Years

APPROVE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) POLICY EFFECTIVE MAY 2, 2023

WHEREAS, the Health Insurance Portability and Accountability Act of 1996 contained in 45 CFR, and subsequent amendment by the Health Information for Economic and Clinical Health Act (HITECH) of 2009, applies to the Warren County Healthcare Plan (the Plan Sponsor); and

WHEREAS, an extensive review of the regulations was conducted and the attached Privacy & Security Policies and Procedures resulted; and

NOW THEREFORE BE IT RESOLVED, to approve and adopt the HIPAA Privacy & Security Policies and Procedures attached hereto and made a part hereto.

M moved for adoption of the foregoing resolution, being seconded by
M . Upon the call of the roll, the following vote resulted:

M
M
M

Resolution adopted this day of May, 2023.

BOARD OF WARREN COUNTY COMMISSIONERS

Tina Osborne, Clerk

HR/ HIPAA Policies and Procedures 2023

C: All Elected Officials and Department Heads
Tammy Whitaker, OMB
Susan Spencer, OMB
Ben Clift, IT
Warren County Data Board

HIPAA

(Health Insurance Portability and Accountability Act of 1996)

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

Revised April 2023

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

A. Permitted Uses and Disclosures of PHI.....- 25 -
B. Disclosures to Plan Sponsor- 33 -
C. Minimum Necessary Standard- 34 -
D. Written Authorizations.....- 36 -
E. Oral or Implicit Permission to Disclose PHI- 38 -
F. De-Identified Information.....- 40 -
G. Requests for Restrictions on Use or Disclosure of PHI.....- 41 -
H. Requests for Confidential Communications- 43 -
I. Right of Access to PHI- 45 -
J. Right to Request Amendment of PHI- 47 -
K. Right to Request an Accounting of Disclosures.....- 50 -
L. Sanctions for Violating the Privacy Rule- 53 -
M. Privacy Complaints.....- 54 -
N. Mitigation of Harm Due to Improper Uses or Disclosures.....- 56 -
O. No Retaliation or Intimidation- 57 -
P. No Waiver of Rights.....- 58 -
Q. Notice of Privacy Practices.....- 59 -

PART III

Security Policies.....- 60 -
A. Risk Analysis- 61 -
B. Risk Management- 62 -
C. Sanctions for Violating the Security Rule- 63 -
D. User Access Management.....- 65 -
E. Authentication & Password Management.....- 68 -
F. Log-In Monitoring.....- 69 -

G. Facility Access Controls.....	- 70 -
H. Workstation Use & Security	- 71 -
I. Device & Media Controls	- 72 -
J. Transmission Security	- 73 -
K. Protection From Malicious Software	- 74 -
L. System Audits, Audit Controls & Activity Review.....	- 75 -
M. Response and Reporting.....	- 76 -
N. Contingency Plan.....	- 78 -
O. Disposal of ePHI.....	- 80 -

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. “Security Officer” means the Warren County Automatic Data Processing Board as defined in Ohio Revised Code 307.847.
13. “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.

14. "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; and
 - Disclosures for law enforcement purposes.
- 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. 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).

- 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:

<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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.
- 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
 - Date and place of birth
 - ABO blood type and rh factor
 - Date and time of treatment
 - Date and time of death, if applicable

color, presence or absence of
facial hair (beard or mustache),
scars, and tattoos

- 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; or
 - The participant or beneficiary will be endangered if the personal representative relationship is recognized.

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 insure 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. 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

G. 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.

H. 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.

I. 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.

J. 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.

K. 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.

L. 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.

M. 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.

N. 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.

O. 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.

P. 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.

Q. 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

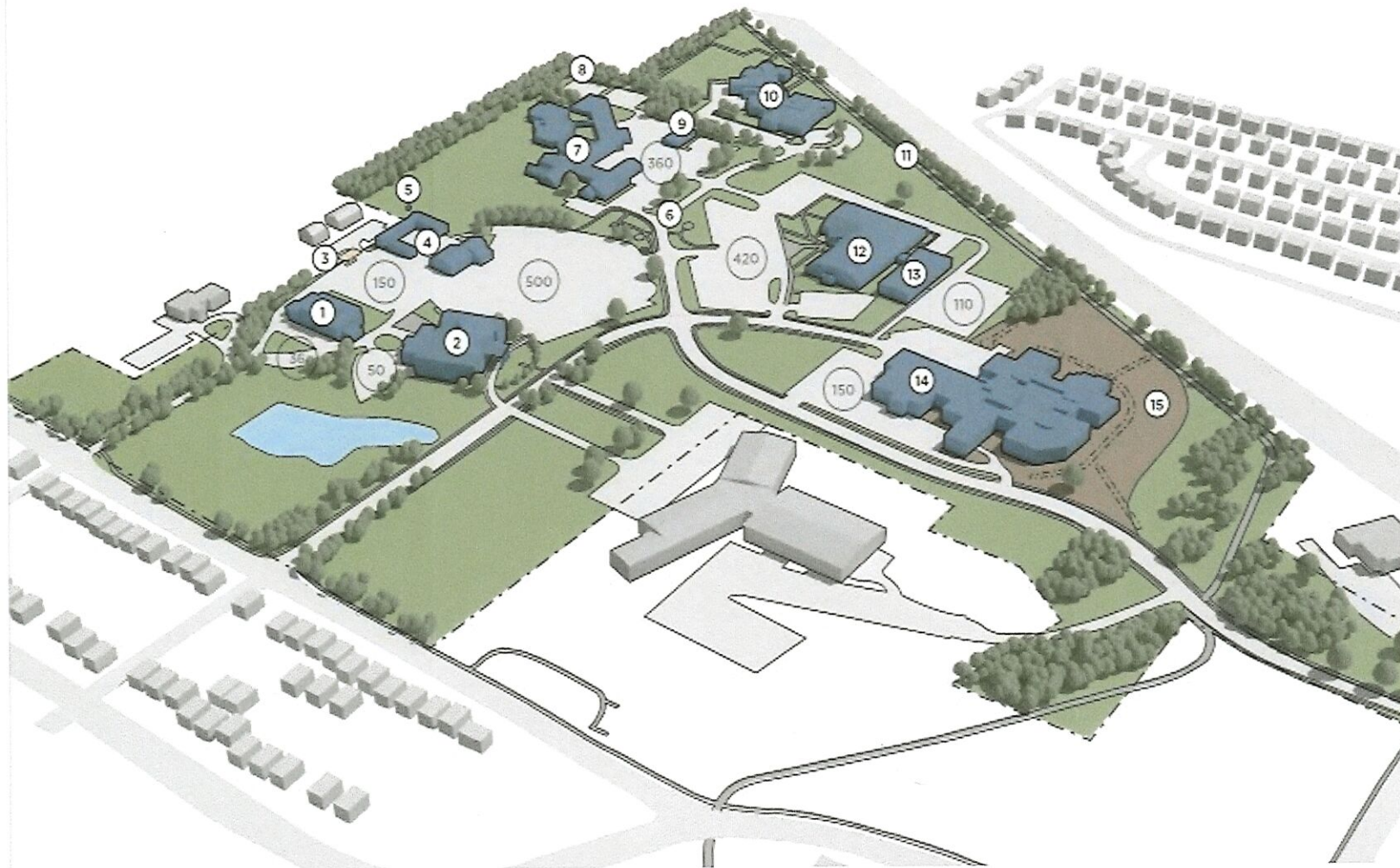
Each Appointing Authority has adopted a retention schedule in addition to the County-wide general retention schedule. ePHI shall be addressed in those policies and shall be retained and/or destroyed pursuant to those policies.

The image is a cover for a document titled "Warren County Master Plan". It features a photograph of the Warren County Courthouse, a large, light-colored building with a prominent dome and a statue on top. The building is partially obscured by trees with vibrant autumn foliage in shades of orange and red. An American flag is visible on a tall pole to the left of the building. The sky is a clear, deep blue. A dark blue horizontal band is superimposed over the middle of the image, containing the title text in a white, elegant serif font.

*Warren County
Master Plan*

EXISTING

JUSTICE DRIVE CAMPUS



- ① Health & Human Services Building
 - ② Administration Building
 - ③ Fueling Station
 - ④ Facilities Management
 - ⑤ Weather Station
 - ⑥ Monuments
 - ⑦ County Court Building & Old Jail
 - ⑧ Impound Lot
 - ⑨ SWAT Garage
 - ⑩ Juvenile Justice Center
 - ⑪ Bike Trail
 - ⑫ Common Pleas Court Building (CPC)
 - ⑬ 520 Justice Office Building
 - ⑭ New Jail & Sheriff's Office
 - ⑮ Drainage
- Ⓜ Parking Counts

PHASE
1A



DEMOLITION

- 1 Demolish the existing Old Jail at 880 Memorial Drive. Note that the County Court Building is to remain and existing infrastructure that feeds County Court must be maintained.
- 2 Construct a replacement SWAT garage and facility at an off-campus location. This 12,000 SF replacement facility will include SWAT vehicle storage, SWAT office and workspace, indoor and/or outdoor firearms training facilities, indoor large County vehicle storage, and secure indoor impounded vehicle storage. This step must be completed before the existing SWAT garage is demolished.
- 3 Demolish the existing SWAT garage.

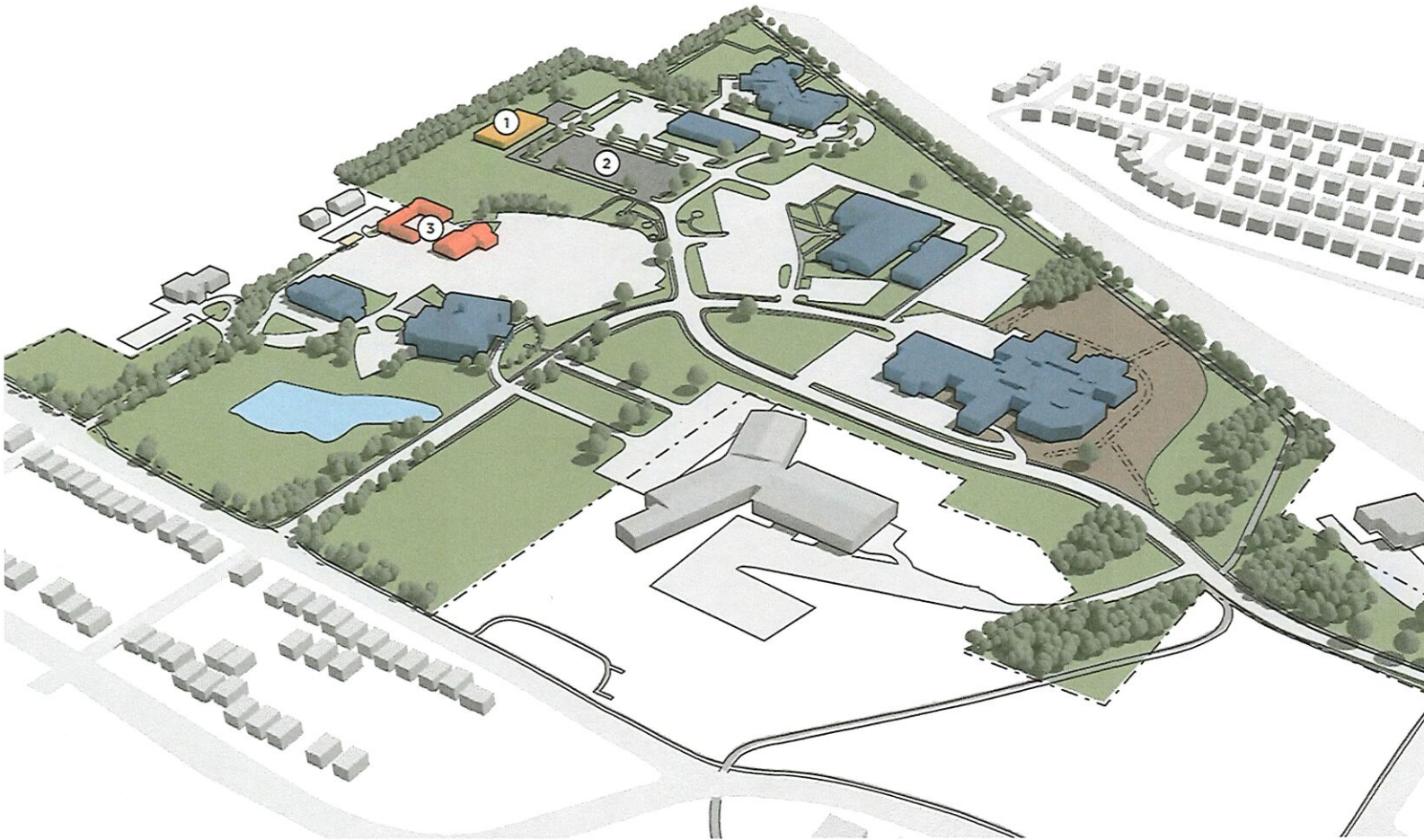
PHASE
1B



COUNTY COURT

- ① Construct a new County Court Building and adjacent parking lot.
- ② Demolish the existing County Court Building.

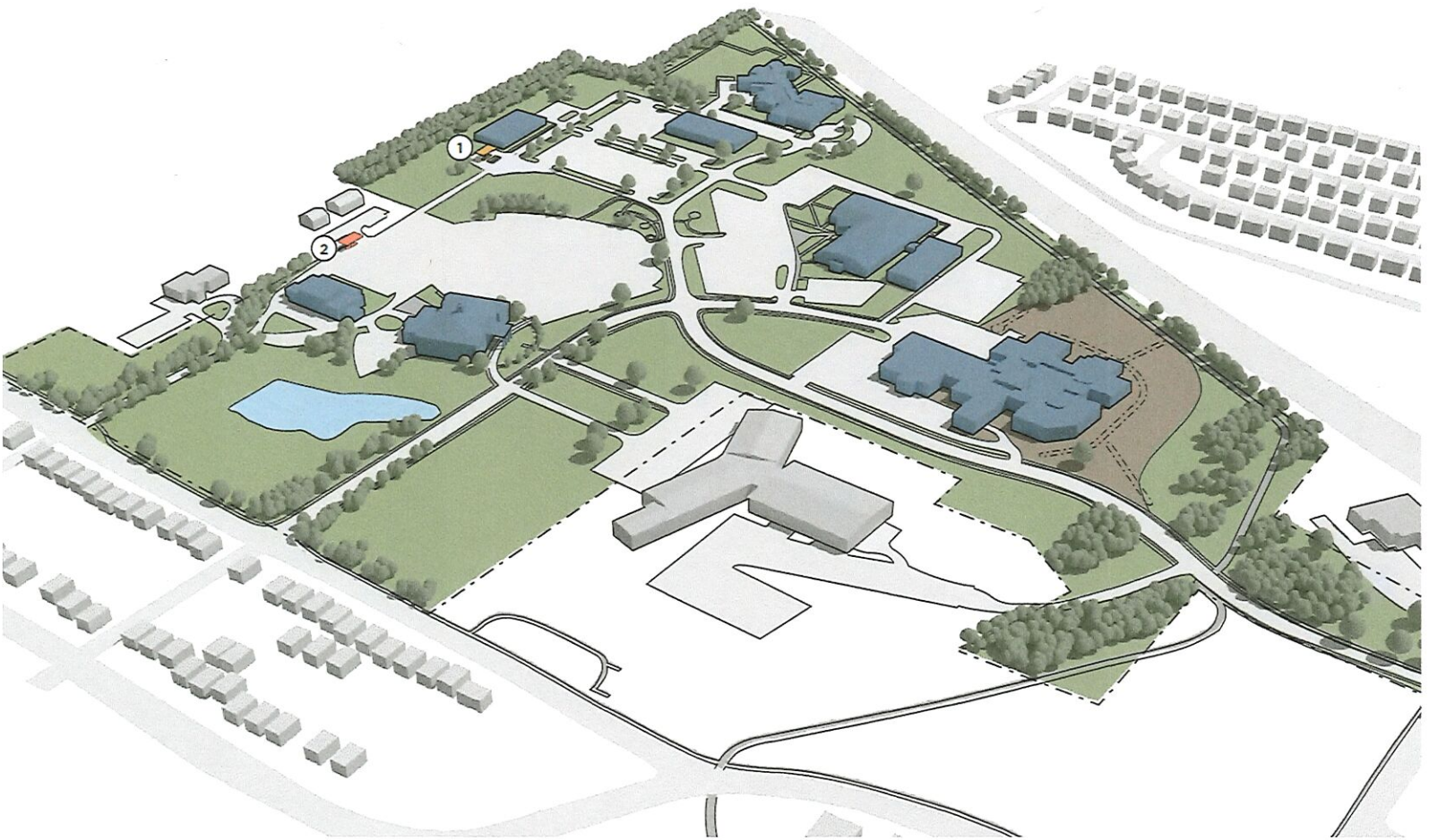
PHASE
1C



FACILITIES MANAGEMENT

- 1 Construct a new 18,000 SF Facilities Management building. This step must be completed before the existing Facilities Management building is demolished.
- 2 Create a new parking lot on the site of the demolished Old Jail and County Court Building.
- 3 Demolish existing Facilities Management building.

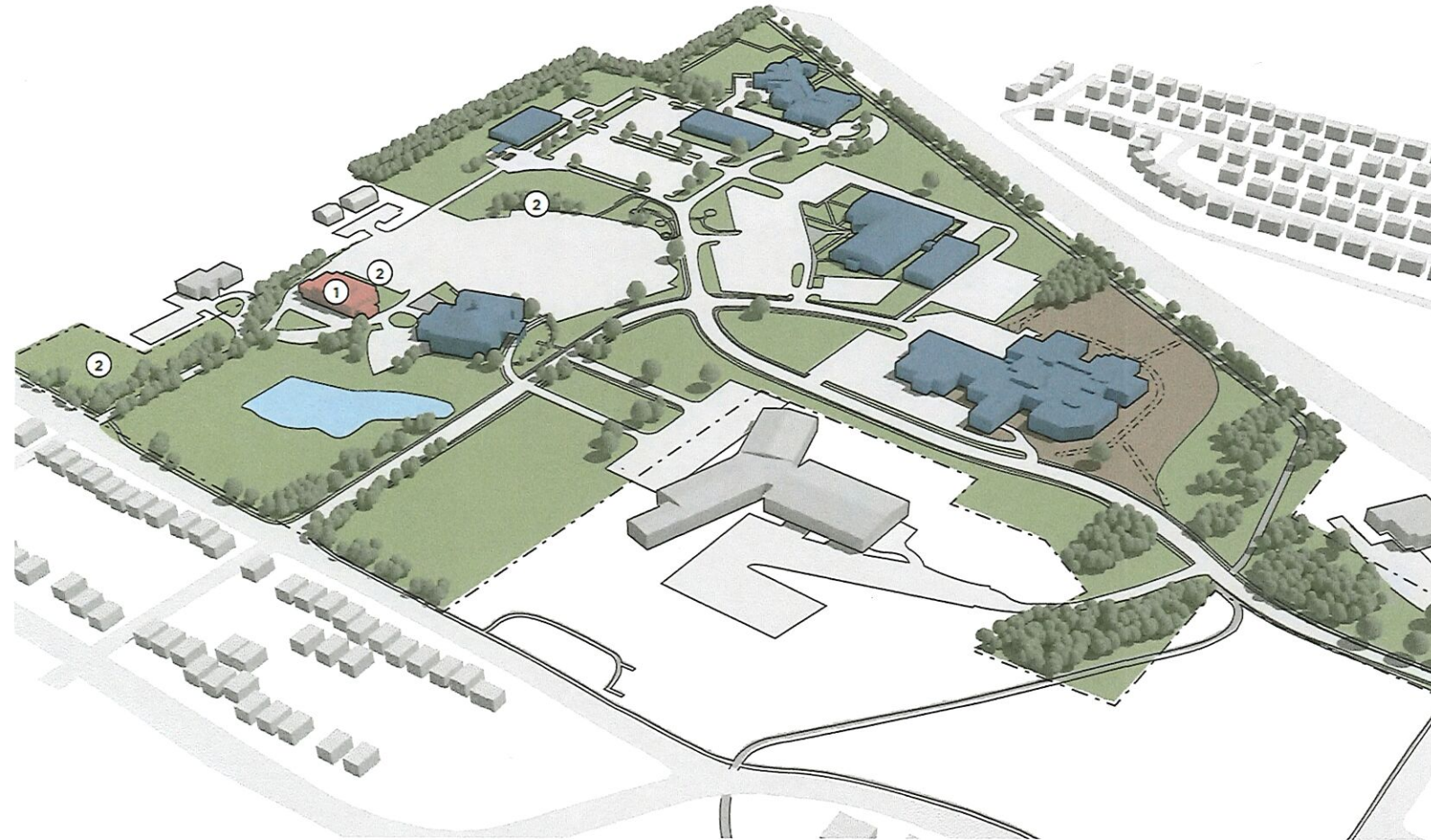
PHASE
1D



FUEL STATION

- ① Construct a new fueling station adjacent to the new Facilities Management building.
- ② Demolish existing fueling station.

END OF
PHASE 1



PLAN PHASE 2

- ① Demolition of Health & Human Services Building.
- ② Creates potential building sites for a new Health & Human Services building and new Board of Elections Building.

Phase 1

1. Demolish the old Jail and SWAT building
 - a. Leave County Court intact
 - b. Build a new tactical response and training facility off campus
2. Construct a new County Court facility, then demolish their current building
3. Construct a new Facilities Management building, then demolish their current building
4. Construct a new Fuel Station, then demolish the current station
5. Plan Phase 2 including a new Health & Human Services building and Board of Elections building.