CHIPPEWA COUNTY

COUNTY BOARD

REGULAR MEETING

NOVEMBER 8, 2022

CHIPPEWA COUNTY COURTHOUSE, RM 302

6:00 PM

NOTE: THE COUNTY BOARD MEETING WILL BE LIVE STREAMED ON YOUTUBE.

During the meeting you can access the video by using the link provided below.

https://youtu.be/HJeSbPnaG9o

1. CALL TO ORDER

2. PLEDGE OF ALLEGIANCE AND MOMENT OF SILENCE

3. ROLL CALL

Attendee Name	Organization	Title	Status	Arrived
Dean Gullickson	Chippewa County	District 5 (Chair)	Present	
Ken Schmitt	Chippewa County	District 3 (Vice-Chair)	Present	
James Flater	Chippewa County	District 1	Absent	
Harold Steele	Chippewa County	District 2	Present	
David Bischel	Chippewa County	District 4	Present	
Glen Sikorski	Chippewa County	District 6	Present	
Jason Bergeron	Chippewa County	District 7	Present	
James Ericksen	Chippewa County	District 8	Present	
Joel Seidlitz	Chippewa County	District 9	Present	
Matthew Peterson	Chippewa County	District 10	Absent	
Roger Calkins	Chippewa County	District 11	Present	
Charles Bomar	Chippewa County	District 12	Present	
Caden Berg	Chippewa County	District 13	Present	
Robert Teuteberg	Chippewa County	District 14	Present	
David Eisenhuth	Chippewa County	District 15	Present	
Ronald McGill	Chippewa County	District 16	Present	
George Rohmeyer	Chippewa County	District 17	Present	
Annette Hunt	Chippewa County	District 18	Present	
Chuck Hull	Chippewa County	District 19	Present	
Dean Mueller	Chippewa County	District 20	Present	
Kari Ives	Chippewa County	District 21	Present	

4. APPROVAL OF AGENDA

others present in room 302 were Lori Zwiefelhofer, Andy Bauer, Toni Hohlfelder, Lynda Schweikert, Todd Pauls, Randy Scholz and Jaclyn Sadler

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Charles Bomar, District 12
SECONDER:	Ronald McGill, District 16
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

5. MEMBERS OF THE PUBLIC WISHING TO BE HEARD

There were no members of the public wishing to be heard.

6. CONSENT AGENDA

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	David Bischel, District 4
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

1. Approval of Minutes

   County Board - Regular Meeting - Oct 11, 2022 6:00 PM

2. AZO 07-22: (Rezone Petition: 2022-0010) Wissota Straits LLC - Rezone

7. REPORTS

A. County Administrator Review and Update

1. Update on Local Assistance and Tribal Consistency Funds
   County Administrator, Randy Scholz, provided an update on the Local Assistance and Tribal Consistency Funds. See attachment.

2. Update on Chippewa County Video Project with CGI Digital
   The County Board of Supervisors watched a video from Lincoln County. County Administrator, Randy Scholz explained the project.

B. Department Reports

C. General Reports

8. BUSINESS ITEMS

1. Res. 56-22: Resolution to Approve Chippewa County Tax Levy to be Collected in 2023 - Randy Scholz

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Robert Teuteberg, District 14
SECONDER:	Ronald McGill, District 16
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

2. Res. 57-22: Resolution to Create the Community Well Drilling Project Ad Hoc Committee of the Land Conservation and Forest Management Committee - Randy Scholz and Lynda Schweikert

   Motion to Amend resolution by Supervisor Steele and Second made by Supervisor Sikorski to add the County Board should also have findings and recommendations. "...shall present its findings and recommendations to the Land Conservation and Forest Management Committee and the County Board after completion of its mission.

   Amendment approved with 10 yes, 9 no, 2 absent. Supervisors voting Yes were Steele, Bischel, Gullickson, Sikorski, Bergeron, Ericksen, Calkins, Eisenhuth, McGill, Mueller. Supervisors voting No were Schmitt, Seidlitz, Bomar, Berg, Teuteberg, Rohmeyer, Hunt, Hull and Ives.

RESULT:	**APPROVED AS AMENDED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	Joel Seidlitz, District 9
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

3. Facility Use Policy Revisions - Second Reading - Larry Ritzinger

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Annette Hunt, District 18
SECONDER:	Caden Berg, District 13
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

4. HR Policy Manual Revisions - Second Reading - Toni Hohlfelder

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	Charles Bomar, District 12
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

5. New HIPPA Policies - Second Reading - Toni Hohlfelder

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	David Bischel, District 4
SECONDER:	Annette Hunt, District 18
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

9. COUNTY BOARD CHAIR APPOINTMENTS

10. COUNTY ADMINISTRATOR APPOINTMENTS

11. AGENDA ITEMS FOR FUTURE CONSIDERATION

Supervisor Hunt would like recognition for the 3 County Volleyball teams (Bloomer, McDonnell and Chi-Hi) for making it to the State Volleyball Tournament.

Supervisor Steele would like to recognize Supervisor Ives for being on a State Committee for Human Services.

12. ADJOURN

meeting adjourned at 6:29 pm

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	James Ericksen, District 8
SECONDER:	Joel Seidlitz, District 9
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	Flater, Peterson

DRAFT

CHIPPEWA COUNTY

COUNTY BOARD

REGULAR MEETING

OCTOBER 11, 2022

CHIPPEWA COUNTY COURTHOUSE, RM 302

6:00 PM

NOTE: THE COUNTY BOARD MEETING WILL BE LIVE STREAMED ON YOUTUBE.

During the meeting you can access the video by using the link provided below.

https://youtu.be/HcM7q9uHaNE

1. CALL TO ORDER

2. PLEDGE OF ALLEGIANCE AND MOMENT OF SILENCE

3. ROLL CALL

Attendee Name	Organization	Title	Status	Arrived	Departed
Dean Gullickson	Chippewa County	District 5 (Chair)	Present		
Ken Schmitt	Chippewa County	District 3 (Vice-Chair)	Present		
James Flater	Chippewa County	District 1	Present		
Harold Steele	Chippewa County	District 2	Present		
David Bischel	Chippewa County	District 4	Present		
Glen Sikorski	Chippewa County	District 6	Present		
Jason Bergeron	Chippewa County	District 7	Present		
James Ericksen	Chippewa County	District 8	Present		
Joel Seidlitz	Chippewa County	District 9	Present		7:19 PM
Matthew Peterson	Chippewa County	District 10	Present		
Roger Calkins	Chippewa County	District 11	Present		
Charles Bomar	Chippewa County	District 12	Present		
Caden Berg	Chippewa County	District 13	Present		
Robert Teuteberg	Chippewa County	District 14	Present		
David Eisenhuth	Chippewa County	District 15	Present		
Ronald McGill	Chippewa County	District 16	Present		
George Rohmeyer	Chippewa County	District 17	Present		
Annette Hunt	Chippewa County	District 18	Present		
Chuck Hull	Chippewa County	District 19	Absent		
Dean Mueller	Chippewa County	District 20	Present		
Kari Ives	Chippewa County	District 21	Present		

others present in room 302 Doug Clary, Randy Scholz, Lori Zwiefelhofer, Andy Bauer, Larry Ritzinger, Toni Hohlfelder, Chris Kowalczyk, Charlie Walker, Brian Kelley, Todd Pauls, Jaclyn Sadler and Traci Bremness

4. APPROVAL OF AGENDA

Minutes Acceptance: Minutes of Oct 11, 2022 6:00 PM (Consent Agenda)

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Harold Steele, District 2
SECONDER:	Ronald McGill, District 16
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

5. MEMBERS OF THE PUBLIC WISHING TO BE HEARD

Chris Kowalczyk spoke to the County Board asking for support for his run for Chippewa County Sheriff

6. CONSENT AGENDA

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	James Flater, District 1
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

1. Approval of Minutes

   County Board - Regular Meeting - Sep 13, 2022 6:00 PM

2. AZO 06 - 22 : 2022-0009 Schumacher Rezone - Woodmohr

7. REPORTS

A. County Administrator Review and Update

B. Department Reports

C. General Reports

8. BUSINESS ITEMS

1. Res. 48 - 22 : Resolution to Sell Highway Property No Longer Needed for Highway Purposes - Brian Kelley

   Highway Commissioner, Brian Kelley, explained the piece of property and the resolution to the board.

   All Supervisors present voted yes, except Supervisor Hunt abstained
   19 Yes, 1 Abstain, 1 Absent

RESULT:	**APPROVED [19 TO 0]**
MOVER:	Glen Sikorski, District 6
SECONDER:	George Rohmeyer, District 17
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Mueller, Ives
ABSTAIN:	Hunt
ABSENT:	Hull

2. Res. 49 - 22 : Resolution to Authorize Use of ARPA Funding for CVIC Improvements - Randy Scholz
County Administrator Scholz spoke on the resolution to use ARPA funding for CVIC improvements

All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Harold Steele, District 2
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

3. Res. 50 - 22 : Resolution to Authorize ARPA Funds for Longevity Rewards - Randy Scholz
County Administrator, Randy Scholz, spoke on the resolution and explained the longevity rewards

All Supervisors present voted yes, except Supervisor Teuteberg abstained. Supervisor Teuteberg stated spouse works for the County.
19 Yes, 1 abstain, 1 absent

RESULT:	**APPROVED [19 TO 0]**
MOVER:	Annette Hunt, District 18
SECONDER:	Charles Bomar, District 12
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSTAIN:	Teuteberg
ABSENT:	Hull

4. 2021-2026 American Rescue Plan Act (ARPA) Plan Amendment - Randy Scholz
County Administrator, Randy Scholz, explained that the passage of the two previous resolutions changes the ARPA plan and would like the board to approve the updated plan

All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Ronald McGill, District 16
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

5. Res. 51 - 22 : Resolution to Amend Resolution 52-21 - Excess Funds from the 2024 Farm Tech Days - Randy Scholz

   County Administrator, Randy Scholz and Chippewa County Economic Development Corporation President, Charlie Walker explained the resolution and miscommunication/misunderstanding from the resolution 52-21 on the excess funds from the 2024 Farm Tech Days

   All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Charles Bomar, District 12
SECONDER:	Robert Teuteberg, District 14
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

6. Res. 52 - 22 : Resolution to Authorize $50,000 from Land Dev. Fund to Stanley Industrial Park - Randy Scholz and Charlie Walker

   County Administrator, Randy Scholz and Chippewa County Economic Development Corporation President, Charlie Walker explained the resolution

   All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	David Bischel, District 4
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

7. Res. 53 - 22 : Resolution to Rescind the Firearms Range Use Policy - Randy Scholz

   County Administrator Scholz spoke on the resolution and explained that since the Firearms Range is closed permanently the policy is no longer needed.

   All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Harold Steele, District 2
SECONDER:	James Flater, District 1
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

8. Ord. 07 - 22 : Ordinance to Amend Ch 70, Art IV, Div 3 Signs, Secs 70-147 to 150 - Second Reading - Doug Clary

   Planning and Zoning Director, Doug Clary was available for any questions. Mr. Clary had explained the ordinance change at the last County Board meeting.

   All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	Ronald McGill, District 16
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

9. Ord. 08 - 22 : Ordinance to Amend Ch 70, Art IV, Div 1, Sec 70-115 Home Occupations - Second Reading - Doug Clary

   Planning and Zoning Director, Doug Clary was available for any questions. Mr. Clary had explained the ordinance change at the last County Board meeting.

   All Supervisors present voted yes

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

10. Facility Use Policy Revisions - First Reading - Larry Ritzinger

    Facilities and Parks Director Larry Ritzinger explained the policy changes

RESULT:	**FIRST READING**	**Next: 11/8/2022 6:00 PM**

11. HR Policy Manual Revisions - First Reading - Toni Hohlfelder
    Human Resources Director, Toni Hohlfelder explained the HR Policy Manual changes

RESULT:	**FIRST READING**	**Next: 11/8/2022 6:00 PM**

12. New HIPAA Policies - First Reading - Toni Hohlfelder
    Human Resources Director, Toni Hohlfelder explained the attached memo that explains the new HIPAA policies

RESULT:	**FIRST READING**	**Next: 11/8/2022 6:00 PM**

9. CLOSED SESSION

1. Closed Session - The County Board will convene in Closed Session pursuant to Wisconsin State Statutes Sec. 19.85(1)(e) "Deliberating or negotiating the purchase of public properties . . . or conducting other specified business, whenever competitive or bargaining reasons require a closed session" (Report on potential site location(s) for future business park).
   The County Board convened to closed session at 6:43 pm

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	Annette Hunt, District 18
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull

2. The County Board will reconvene to open session to continue with the agenda
   The County Board returned to open session at 8:08 pm.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull
EXCUSED:	Seidlitz

10. COUNTY BOARD CHAIR APPOINTMENTS

11. COUNTY ADMINISTRATOR APPOINTMENTS

1. County Administrator Appointment - Crime Prevention Funding Board

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	Charles Bomar, District 12
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull
EXCUSED:	Seidlitz

12. AGENDA ITEMS FOR FUTURE CONSIDERATION

13. ADJOURN

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Annette Hunt, District 18
SECONDER:	Ken Schmitt, District 3 (Vice-Chair)
AYES:	Gullickson, Schmitt, Flater, Steele, Bischel, Sikorski, Bergeron, Ericksen, Peterson, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Mueller, Ives
ABSENT:	Hull
EXCUSED:	Seidlitz

STATEMENT OF EXPLANATION

Amendatory Zoning Ordinance No. 07 - 22

AZO 07-22: (REZONE PETITION: 2022-0010) WISSOTA STRAITS LLC - REZONE

Comprehensive zoning consists of written text (commonly referred to as the zoning ordinance) and an official zoning map. The zoning ordinance is a guideline for permitted and conditional uses, which are separated into zoning classifications or districts. The zoning map shows how a town board has designated the particular zoning classifications or districts to parcels of land within their particular jurisdiction. A rezone is where a property owner or other authorized entity seeks to amend the official zoning map, which would allow a use that is currently not permitted on the parcels of land based on the existing zoning classification or district. This is referred to as a zoning map amendment or "rezoning". The requested rezoning change may not be granted if it does not fit with the comprehensive plan and community goals for the respective town and county.

LEGAL DESCRIPTION

Parcel Number 22808-1031-00020002, which is located in the NE 1/4 of the SW 1/4, Section 10, Township 28 North, Range 08 West. Town of Lafayette. Physical Address: Vacant Land.

From: Residential 2 - Twin Home **To:** Residential 2

Amendatory Zoning Ordinance No. 07 - 22

AZO 07-22: (REZONE PETITION: 2022-0010) WISSOTA STRAITS LLC - REZONE

Zoning Petition No:	2022-0010
Town Board Action:	October 17, 2022, Approve
Planning & Zoning Committee Public Hearing:	October 20, 2022
Recommendation from Planning & Zoning Committee:	Approve as presented

Comments/Conditions: None

The Chippewa County Board of Supervisors does ordain as follows:

That the Zoning maps, dated 1974 and land description listing the boundaries of the eleven zoning districts, and referred to in Chapter 70-61 of the Chippewa County Zoning Ordinance, adopted on February 14, 2006, to be amended as follows:

LEGAL DESCRIPTION

Parcel Number 22808-1031-00020002, which is located in the NE 1/4 of the SW 1/4, Section 10, Township 28 North, Range 08 West. Town of Lafayette. Physical Address: Vacant Land.

From: Residential 2 - Twin Home **To:** Residential 2

The new map, now dated November, 2022 and land description are made a part of the Zoning Ordinance. All notations, references and other information shown upon said "zoning map" November, 2022 and land description shall be as much a part of this Ordinance as if the matter and things set forth by said map and land description were fully described herein.

This Ordinance shall become effective upon passage.

Dated this **8th** day of **November, 2022**

RESULT:	**APPROVED BY CONSENT VOTE [UNANIMOUS]**
MOVER:	David Bischel, District 4
SECONDER:	James Ericksen, District 8
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	James Flater, Matthew Peterson

(Publish – Chippewa Herald – October 6 and October 13, 2022)

CHIPPEWA COUNTY PLANNING & ZONING COMMITTEE
NOTICE OF PUBLIC HEARING
STATE OF WISCONSIN

PUBLIC NOTICE is hereby given to all persons in the County of Chippewa, Wisconsin, that a public hearing will be held on **October 20, 2022** beginning at **4:30 PM** at the Chippewa County Courthouse, Room 302, 711 N Bridge Street, Chippewa Falls, Wisconsin relative to the following request:

Rezone Petition: 2022-0010
Petitioner: Wissota Straits LLC **Agent:** David Christoffel
Parcel Number 22808-1031-00020002, which is located in the NE ¼ of the SW ¼, Section 10, Township 28 North, Range 08 West, Town of Lafayette. Physical Address: Vacant land

From: Residential 2-Twin Home **To:** Residential 2

Specific information regarding these public hearings can be obtained at the Chippewa County Department of Planning & Zoning. All persons interested are invited to attend these hearings.

Dated this 3rd day of **October**, 2022

Douglas Clary, Director
Department of Planning & Zoning
Chippewa County

CHIPPEWA COUNTY
DEPARTMENT OF PLANNING & ZONING

• 711 North Bridge Street, Chippewa Falls, WI 54729 • Phone:715.726.7940 • Fax:715.726.4596 • www.co.chippewa.wi.us •

Land Management | Land Planning | Land Records & G.I.S. | POWTS & Wells

Date: October 3, 2022

To: Property Owner(s)

From: Douglas Clary, Director

Re: Public Meetings & Public Hearing

Dear Property Owner(s):

The Chippewa County Department of Planning & Zoning has received a rezone petition for a parcel of land that is located either adjacent to or in the vicinity of property owned by you. You are receiving this notice because your property has been determined to be within the legal public hearing notification distance per county and state requirements. I have enclosed a map identifying the location of the parcels associated with the rezone petition. If you have any questions regarding this rezone petition, please contact me at (715) 726-7941.

REZONE PETITION: #2022-0010
Property Owner: Wissota Straits LLC **Agent:** David Christoffel
Parcel number 22808-1031-00020002, which is located in the NE ¼, of the SW ¼, Section 10, Township 28 North, Range 08 West. Town of Lafayette.

From: Residential 2-Twin Home **To:** Residential 2

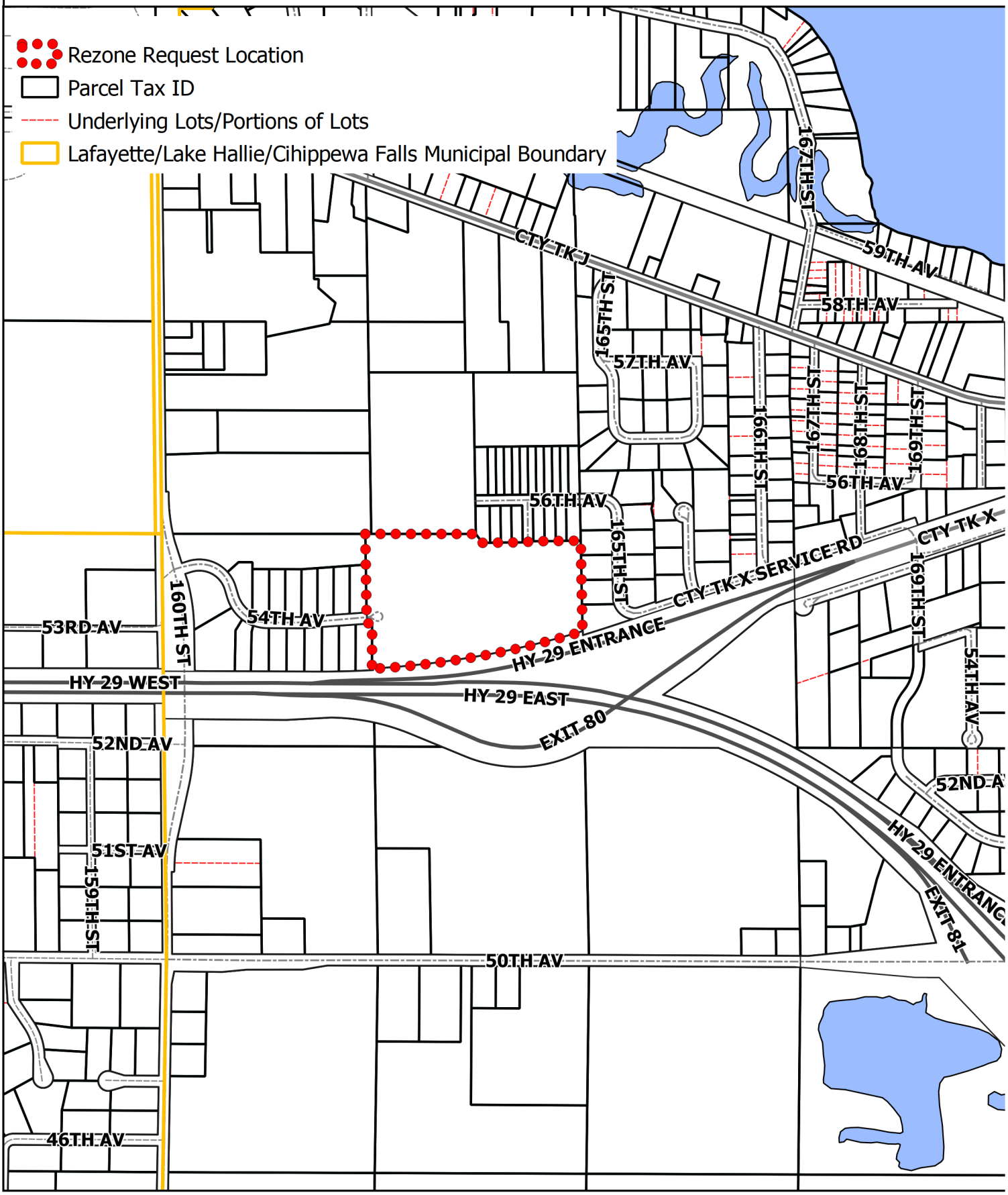
Purpose: Proposed subdivision – Two-Family Dwellings

Lafayette Town Park, Recreation & Land Use Planning Commission (PRLPC):
The PRLPC will **REVIEW** this request on **October 10, 2022** at approximately **7:00 PM**. The PRLPC will make an **ADVISORY** recommendation to the Lafayette Town Board to approve or disapprove. This meeting will be held at the Lafayette Fire Station, 5855 197th Street, Chippewa Falls, Wisconsin 54729.

Lafayette Town Board:
The Town Board will **REVIEW** this request on **October 17, 2022** at approximately **7:00 PM**. The Town Board will forward an **ADVISORY** recommendation to the Chippewa County Planning & Zoning Committee to approve, disapprove or approve with modification(s) and/or condition(s). This meeting will be held at the Lafayette Town Hall, 5765 197th Street, Chippewa Falls, Wisconsin 54729 or via telephone.

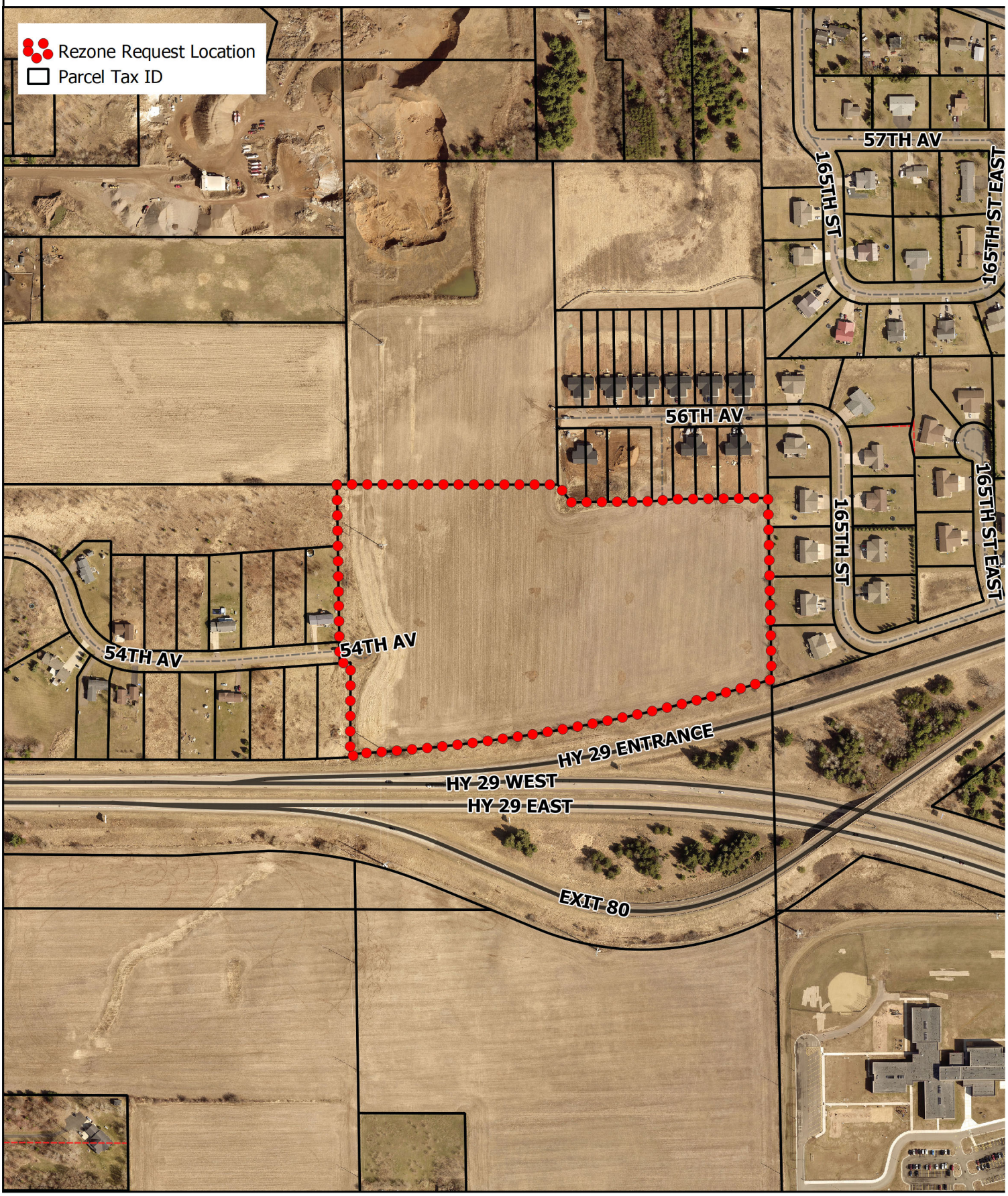
Chippewa County Planning & Zoning Committee:
The Chippewa County Planning & Zoning Committee will hold a **PUBLIC HEARING** for this petition on **October 20, 2022** at **4:30 PM** in the Chippewa County Courthouse, Room 302, 711 N Bridge Street, Chippewa Falls, Wisconsin. The Committee will make a determination on the petition to approve, disapprove or approve with modification(s) and/or conditions. If the Planning & Zoning Committee approves or approves with modification, the petition will be forwarded to the County Board meeting on **November 8, 2022** at **6:00 PM** for their consideration. If the Planning & Zoning Committee disapproves, the petition will fail.

2022-0010 Wissota Straits LLC - Rezone Request - Location Map



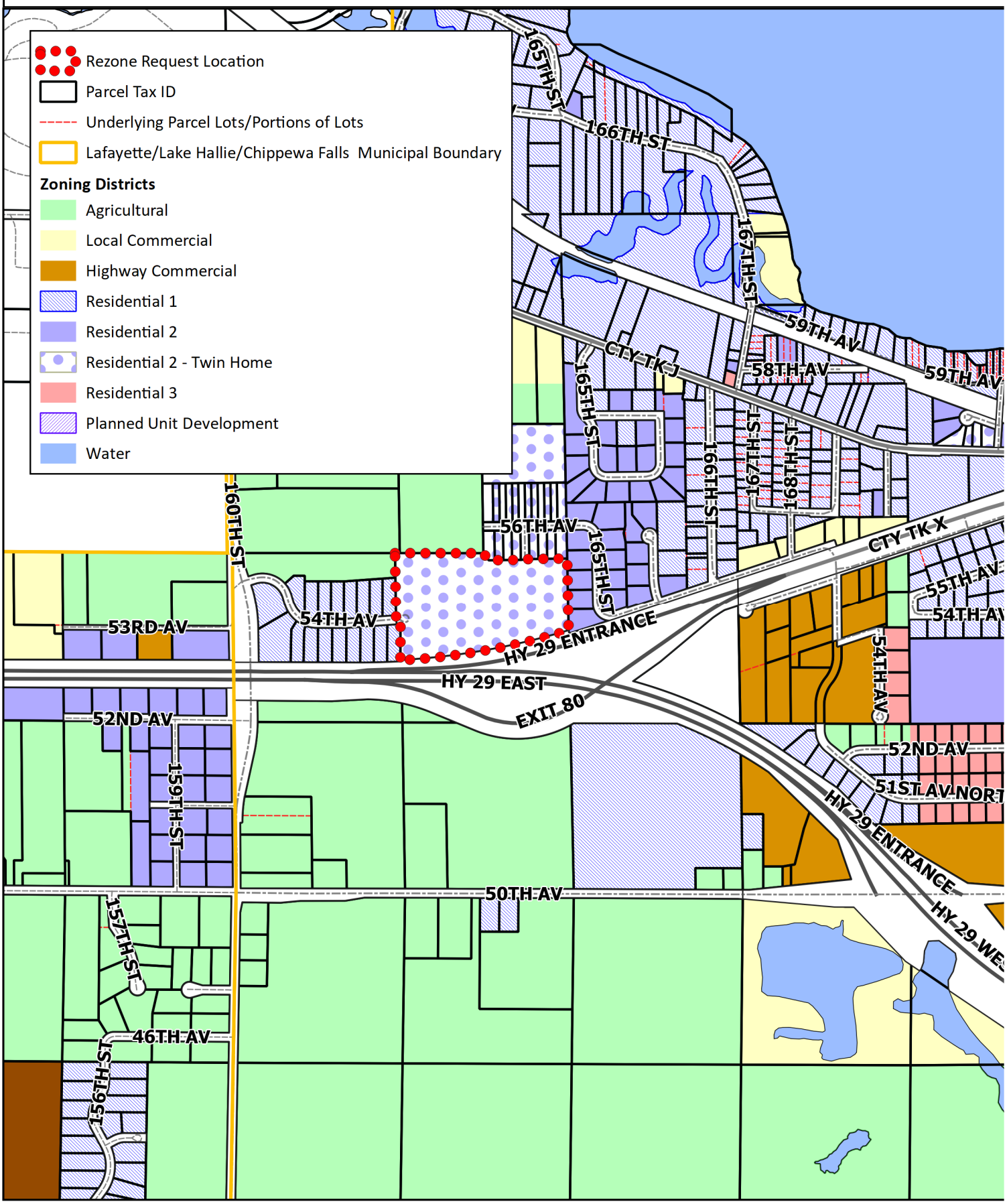
Produced on October 3, 2022 by the Chippewa County Department of Planning & Zoning and is for reference purposes only.

2022-0010 Wissota Straits LLC - Rezone Request - Aerial (2021)



Produced on October 3, 2022 by the Chippewa County Department of Planning & Zoning and is for reference purposes only.

2022-0010 Wissota Straits LLC - Rezone Request - Zoning Districts



Produced on October 3, 2022 by the Chippewa County Department of Planning & Zoning and is for reference purposes only

CHIPPEWA COUNTY
DEPARTMENT OF PLANNING & ZONING
• 711 North Bridge Street, Chippewa Falls, WI 54729 • Phone:715.726.7940 • Fax:715.726.4596 • www.co.chippewa.wi.us •

2022 Rezone Application

Comprehensive zoning consists of written text (commonly referred to as the zoning ordinance) and an official zoning map. The zoning ordinance is a guideline for permitted and conditional uses, which are separated into zoning classifications or districts. The zoning map shows how a town board has designated the particular zoning classifications or districts to parcels of land within their particular jurisdiction. A **REZONE** is where a property owner or other authorized entity seeks to amend the official zoning map, which would allow a use that is currently not permitted on the parcels of land based on the existing zoning classification or district. This is referred to as a zoning map amendment or "rezoning". The requested rezoning change may not be granted if it does not fit with the comprehensive plan and community goals for the respective town and county.

SECTION I: Parcel Owner Information			**SECTION II: Agent Information**		
Name: Wissota Straits LLC			**Name:** David Christoffel		
Mailing Address: 9796 20th Street			**Mailing Address:** 9796 20th Street		
City: Colfax	**State:** WI	**Zip:** 54730	**City:** Colfax	**State:** WI	**Zip:** 54730
Telephone: 715-704-0250			**Telephone:** 715-704-0250		
Email Address (Required): davidchristoffel2247@gmail.com			**Email Address (Required):** davidchristoffel2247@gmail.com		
SECTION III: Parcel Information					
Town of: Lafayette			**Property Address:** None		
Parcel Number(s): 22808-1031-00020002			**City:** Chippewa Falls	**State:** WI	**Zip:** 54729
Existing Zoning District(s): R2-TH			**Proposed Zoning District(s):** R2		

GENERAL DIRECTIONS:

1. **Complete** this Application form and the required four (4) parts:
   - ☐ Part 1: General Questions related to the request
   - ☐ Part 2: Planning & Zoning Committee Schedule - 2022
   - ☐ Part 3: General Rezoning Process
   - ☐ Part 4: Applicant Acknowledgement/Signature
2. **Submit** the completed application, all required information and a **$350.00** public hearing fee (Make check payable to: Chippewa County Treasurer) by the deadline (as listed in Part 2) to the Chippewa County Department of Planning & Zoning, Room 009, 711 N. Bridge Street, Chippewa Falls, Wisconsin 54729.
3. **Make arrangements** to attend or have a representative attend any local town plan commission or town board meetings, and the required Planning & Zoning public hearing. This presence is needed so that questions can be answered and concerns addressed.

FOR DEPARTMENT OF PLANNING & ZONING STAFF USE:		
Receipt Number: 21160	**Appeal Number:** 2022-0010	**Public Hearing Date:** 10-20-2022

Chippewa County – 2022 Rezone Application

Once the completed application is received, the Department will prepare a public hearing notice and publish it within the Chippewa Herald. The public hearing notice will include the location and time of the required public hearing before the Chippewa County Planning & Zoning Committee. In addition, your neighbors, the Town Board and any appropriate county or state agencies will be notified. At the public hearing, any party may appear in person or may be represented by an agent or attorney to present information to the Planning & Zoning Committee in support or opposition of the rezone request.

Part 1: General Questions. Please use a separate 8.5" x 11" sheet to answer these questions.

1. As the applicant, do you have legal title to the parcel(s)? If you **do not** have legal title to the property, please have the property owner sign this application.
2. Identify the parcel(s) that are or will be part of this rezone request. If needed, an additional sheet listing those parcels can be attached.
3. Describe the present and, if known, any proposed improvements on each parcel of land.
4. Explain why you are requesting to rezone of each parcel. Please identify the proposed use of each parcel.
5. Explain the compatibility of your proposed use(s) with the existing use(s) on adjacent parcels and those in the vicinity of this parcel(s).
6. Discuss any additional issues you feel that supports the consistency of your proposed use with County ordinances and plans as well as any Town ordinances or plans.

Be prepared to give a detailed presentation when called upon at the public hearing before the Planning and Zoning Committee. Prepare an outline of your proposal, something similar to a "business plan", detailing for the Planning & Zoning Committee your proposal. Include any documentation you feel is necessary as part of your presentation in defining your proposal for the Committee and possibly the County Board. It is vital to your application to consult with professionals you feel may be able to assist with your application (i.e. surveyor, attorney, engineer, etc.)

Part 2: Planning & Zoning Committee Schedule - 2022

Applications will not be placed on the appropriate agenda unless they are properly completed and include **ALL** required supporting information or documents **and** payment of the public hearing fee. Applicants are encouraged to consult with staff of the Department of Planning & Zoning prior to the filing of the application. This is an important step to insure that all pertinent issues are identified and to determine what information in addition to the application forms might be necessary in order for the department to accept and process your application. Please CIRCLE or HIGHLIGHT the meeting you intend on attending:

Application Deadline: 12:00 Noon	Public Hearing
December 22, 2021	January 20, 2022
January 27, 2022	February 24, 2022
February 24, 2022	March 24, 2022
Due to the County Board Reorganization, the April meeting will not occur.	
April 21, 2022	May 19, 2022
May 26, 2022	June 23, 2022
June 23, 2022	July 21, 2022
July 21, 2022	August 18, 2022
August 25, 2022	September 22, 2022
September 22, 2022	October 20, 2022
October 20, 2022	November 17, 2022
November 17, 2022	December 15, 2022

*Note: Applications and all supporting information are due at **12:00 Noon** on the designated date.*
Note: Typically, the Planning & Zoning Committee meetings start at 4:30 PM on the designated dates above.
Note: Deadlines, public hearing dates and times after April 1st are subject to change due to the County Board Reorganization.

Part 3: General Rezoning Process:

(A) The rezone application is filed with the Department of Planning & Zoning. This includes the legal description of the parcels to be rezoned, a written statement addressing the questions as listed in Part 1 and any other information your feel will aid in a decision on this request.

(B) The Town Board will be notified of the rezone application. The Town Board can recommend approval or denial of a rezoning request. If the Town Board denies a rezone request, the Planning & Zoning Committee can only recommend an approval with modification to the rezone request or deny the rezone request.

(C) A Class 2 Public Hearing Notice will be published in the Chippewa Herald detailing the request and the date and time of the Public Hearing.

(D) Property owners of the land and those property owners within 400' (or maybe a greater distance) of the requested rezone change are notified directly by mail as well as the Town Board Chair and Town Clerk. The notice to the property owners will generally contain a portion of the public hearing notice and information pertaining to meetings to be held at the Town level (plan commission, town board, etc) as well as the Public Hearing in front of the Planning & Zoning Committee.

(E) General maps (location map, aerial view and existing zoning districts map) will be prepared for the request by the Department.

(F) A department staff report is prepared and sent to the Planning & Zoning Committee, while comments from the general public are solicited.

(G) Following the Public Hearing, the Planning & Zoning Committee will make a motion to either approve, approve with modification or deny the rezoning request. If the rezone request receives an approval or approval with modification an ordinance amendment will be prepared and placed on the next County Board meeting agenda for their approval.

(H) If the County Board approves the rezone and the town board files an objection to the approval, the town board will then have 45 days to veto the rezone request following the applicable state statutes.

(I) If the rezone request receives County Board approval, the final step is the publication of the amendment in the Chippewa Herald. Once published, the zoning district amendment takes effect. The entire process from application deadline to final publication can take two months or more to complete depending upon the scheduling of hearing dates.

Part 4: Applicant Acknowledgement/Signature

This application must be signed by the property owner or in case of an agreement to purchase the property, a letter from the property owner acknowledging the potential buyer is seeking the rezone.

- I certify that the information I have provided in this application is true, accurate and complete.
- I or a representative will have an opportunity to present to the Planning & Zoning Committee information in favor of this request.
- I have the authority to allow the staff of the Department of Planning & Zoning and Planning & Zoning Committee member's access to the property to conduct necessary inspections related to this request.
- I understand that I cannot speak to any member of the Planning & Zoning Committee about this application, except at the public hearing.
- I understand that I cannot direct any written communication about this application to a member of the Planning & Zoning Committee, unless I also file a copy with the Department of Planning & Zoning and direct additional copies to each person who has registered an interest in this application.
- I also understand that if I or my representative fail to appear in front of the Planning & Zoning Committee during the designated public hearing or my failure to observe the above mentioned rules, my request may be **DENIED**.

Signed: _____ Date: 9/20/2022
Owner/Agent

Part 5: Planning & Zoning Department Mailing List

Applicant
Property Owner Owners within 400'
Planning & Zoning Committee Members
Town Board Chair & Clerk
County Board Supervisor
News Media
Others
Wisconsin DNR
US Army Corp of Engineers
Wisconsin DOT

Chippewa County Rezone Application

Part 1: General Questions

1. As the applicant, do you have legal title to the parcels? **Yes**

2. Identify Parcels: **Included in Section III, Page 1 of application**

3. Describe present and, if known, any proposed improvements on each parcel of land. **None. Cropped farmed currently.**

4. Explain why you are requesting to rezone each parcel. **Applicant is intending on rezoning the parcel to develop a high quality two-family dwelling community.**

5. Explain the compatibility of your proposed use with the existing uses on adjacent parcels and those in the vicinity of these parcels: **Neighboring properties are residential or agricultural in nature and the proposed use is consistent with surrounding properties which includes two-family dwelling land directly adjacent and East of subject parcel, two-family twinhome dwelling land directly North, single family dwelling land adjacent to West, and highway commercial directly South of subject parcel.**

6. Discuss any additional issues you feel that support your request: **None**

Part 2: Legal Description

EXHIBIT A

Legal Description:

The NE 1/4 of the SW 1/4 of Section 10, Township 28 North, Range 8 West, Town of Lafayette, Chippewa County, Wisconsin;

EXCEPT Lands conveyed for Highway Purposes;

EXCEPT Lands lying South of State Highway 29;

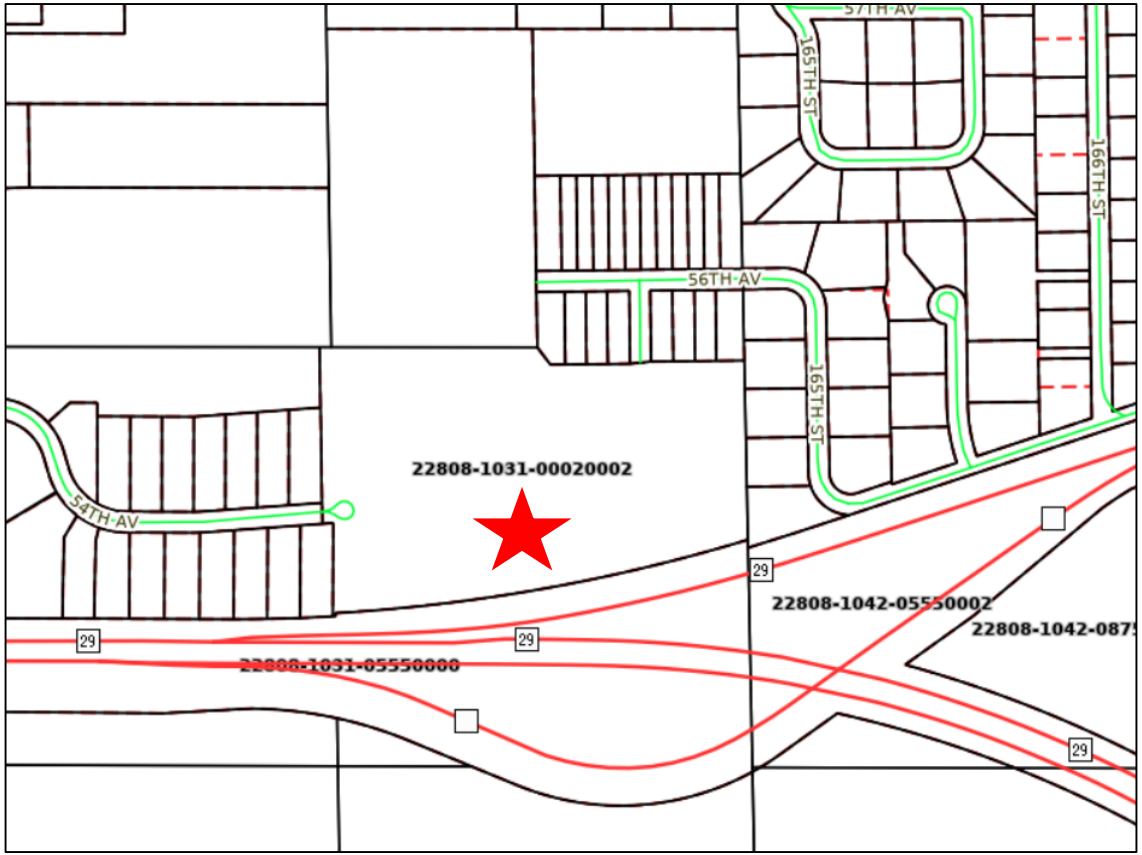
EXCEPT Lands platted as Lafayette Point Addition;

AND that part of the NW 1/4 of the SW 1/4 of Section 10, Township 28 North, Range 8 West, Town of Lafayette, Chippewa County, Wisconsin lying East of Lot 10, Highview Estate, and North of 54th Avenue, extended to the North line of the NW 1/4 of the SW 1/4.

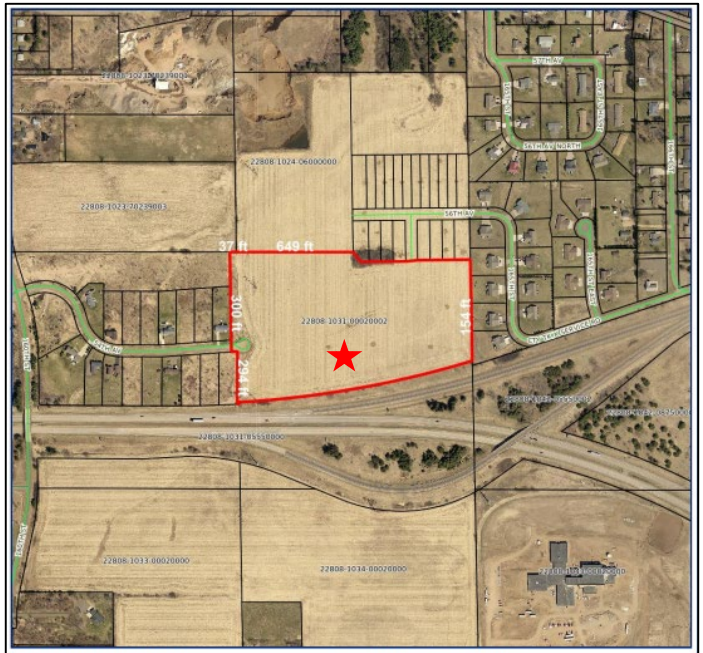
22 Acre
Wissota Meadows

09/20/2022

22 Acre Parcel Identification



22 Acre Parcel Report

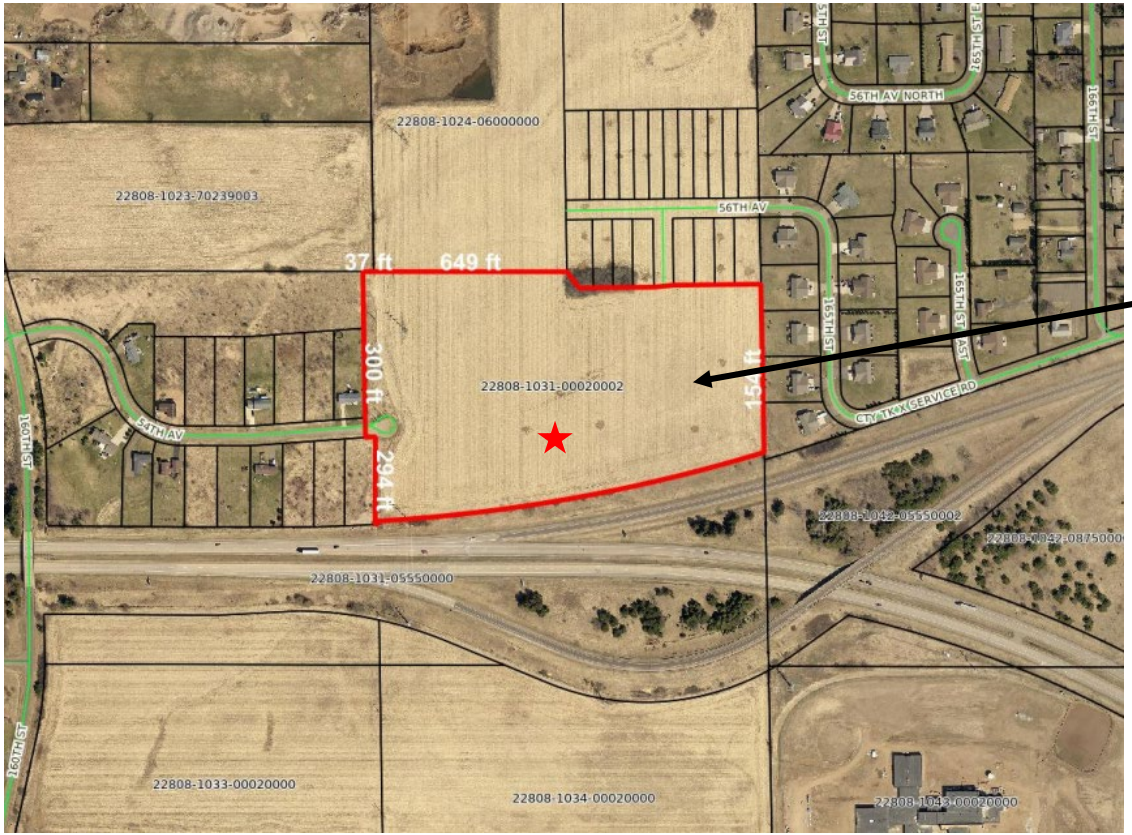


PIN: 22808-1031-00020002 Computer Number: 034-1245
Owner Name: WISSOTA STRAITS LLC
Owner Address: 9796 20TH ST
Owner Address: COLFAX WI, 54730
Physical Address:
GIS Acres: 22.2 Deed Acres: 22.2
School Code: 1092
Assessed Value: 3700 Fair Market Value: 5600
Description: NE SW EX STATE HWY 29 - SEE COMP #1249 & EX LYING S OF HWY 29 & EX LAFAYETTE POINTE & INC PART OF THE NW SW LYING E OF LOTS 9 & 10 HIGHVIEW ESTATES AND N OF 54TH AVE, EXTENDING TO THE N LIN NW SW

Scale = 1":470'
Printed 09/13/2022

Disclaimer: This map is a compilation of records as they appear in the Chippewa County Offices affecting the area shown and is to be used only for reference purposes.

Current Site Use



Parcel:
22808-1031-00020002

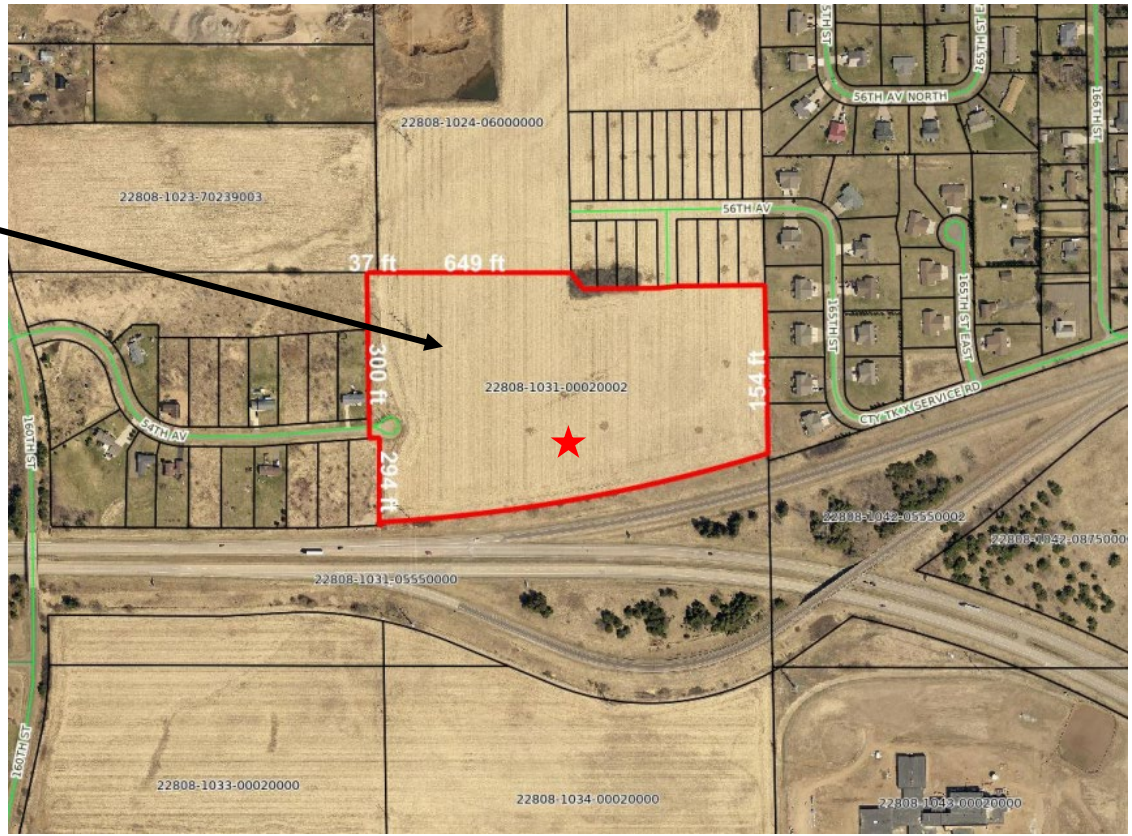
Currently used as rotational cropland

2022 valuations	
Class	Acres
G4 - AGRICULTURAL	21.200
G5 - UNDEVELOPED LAND	1.000
ALL CLASSES	22.200

Proposed Rezone & Site Use

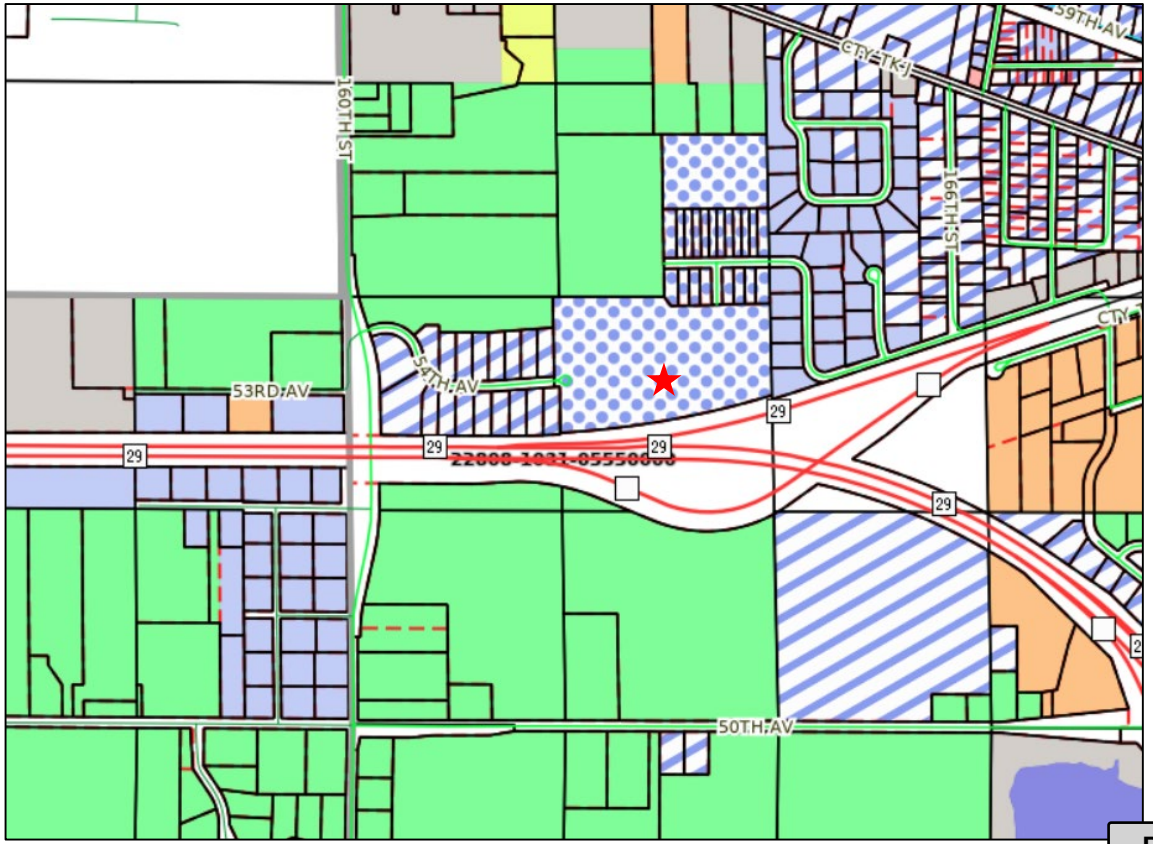
Parcel:
22808-1031-00020002

Rezone from R2-TH to R2

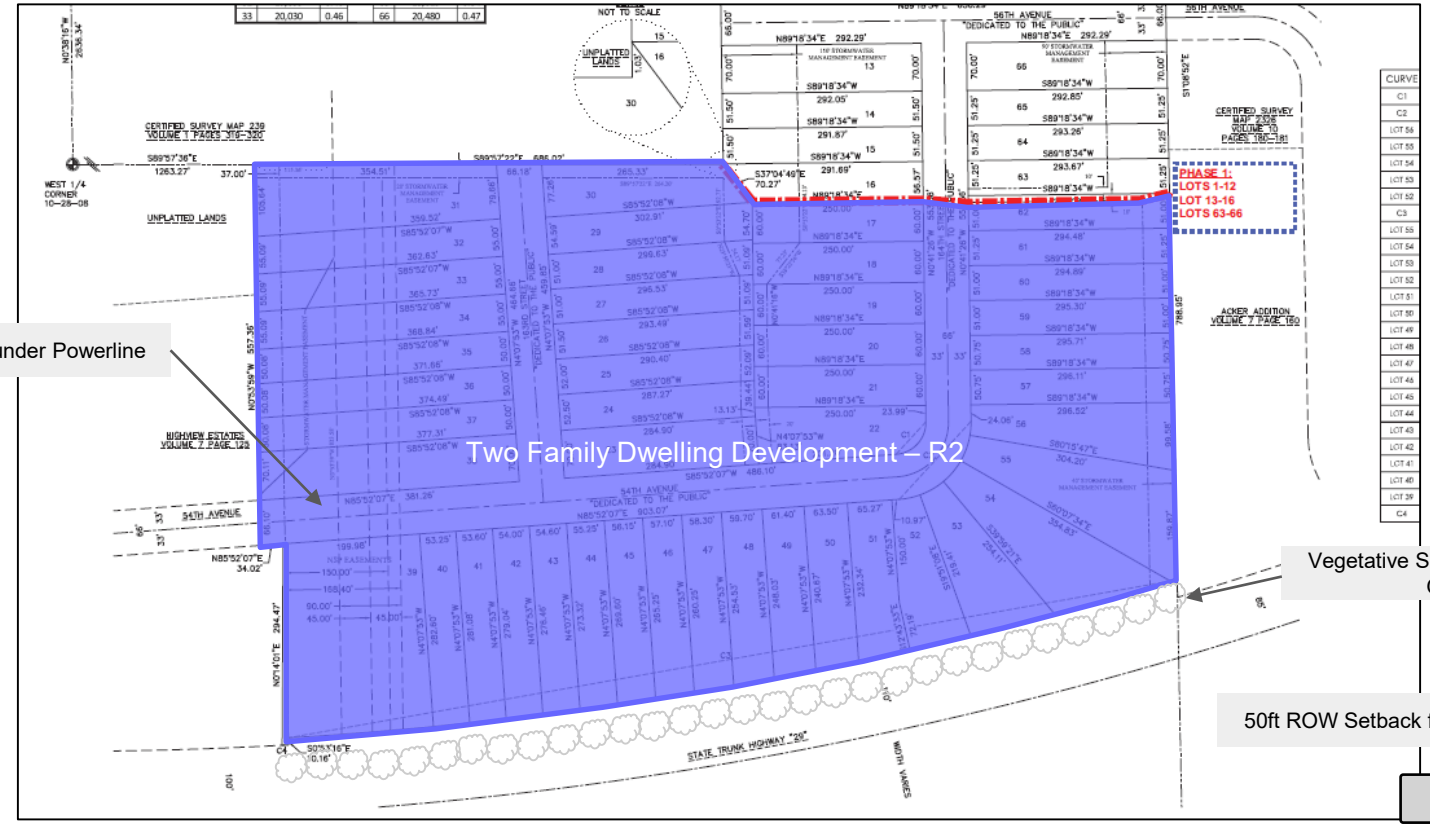


R2 Compatibility with Surrounding Sites

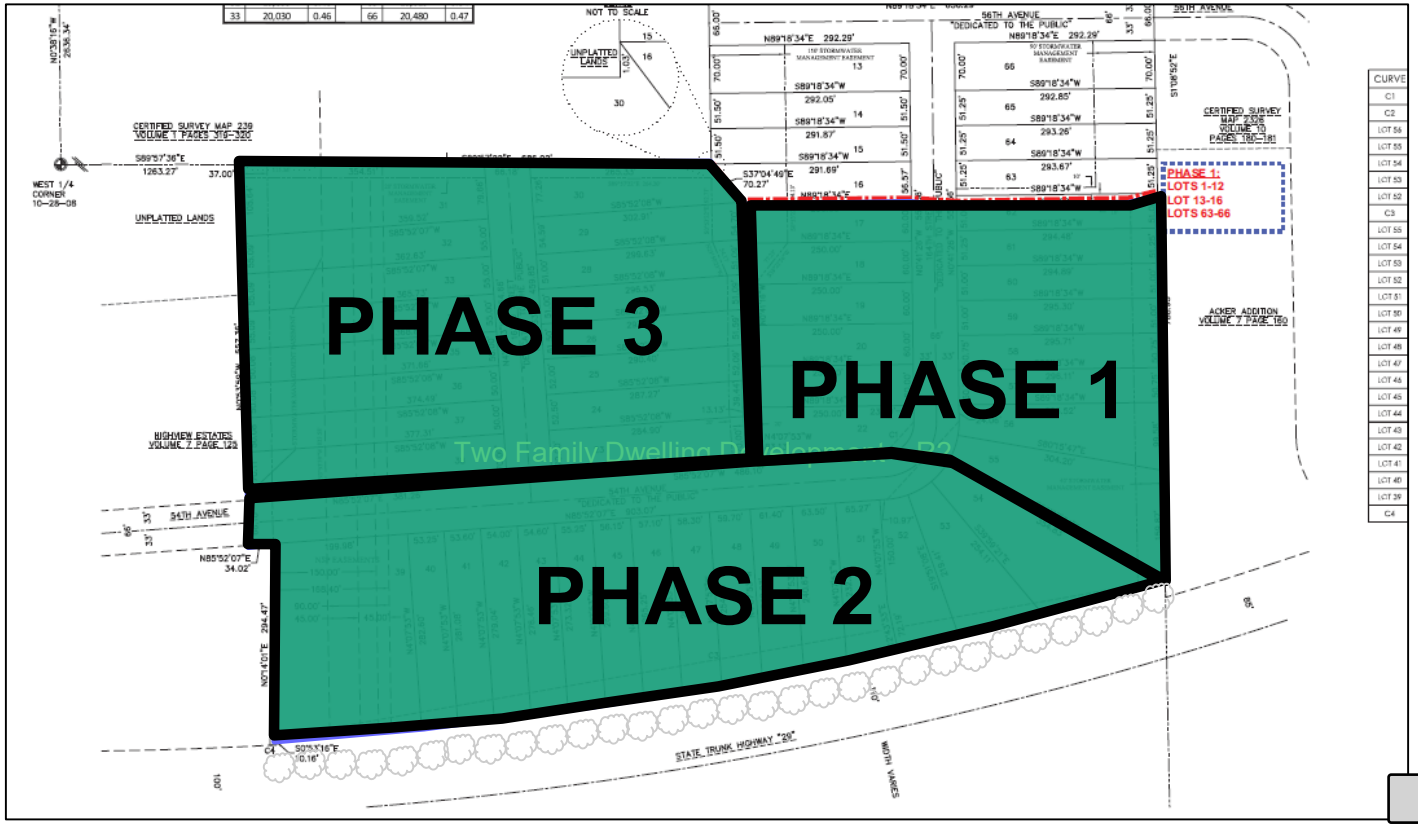
- Agriculture
- Residential 1
- Residential 2
- Residential 2-Twin Home
- Residential 3
- Planned Unit Development
- Local Commercial
- Highway Commercial
- Industrial
- Recreational
- Conservancy
- Public Conservancy
- Public Institutional



Site Plan Overview



Site Plan with Phases



Department of Administration

Randy B. Scholz, County Administrator

October 5, 2022

TO: County Board of Supervisors

FR: Randy Scholz

RE: Local Assistance and Tribal Consistency Funds (LATCF)

Good afternoon,

We were recently informed the U.S. Department of the Treasury has released Local Assistance and Tribal Consistency Funds (LATCF). The LATCF delivers $2 billion to eligible Tribal governments and eligible revenue sharing counties as a general revenue enhancement program. The American Rescue Plan Act (ARPA) appropriates $750 million to allocate and pay to eligible revenue sharing counties for each of fiscal year 2022 and 2023.

Recipients have broad discretion on the use of funds. Specifically, the statute permits recipients to use funds for any governmental purpose other than lobbying activity. Recipients may treat these funds in a similar manner to how they treat funds generated from their own revenue. All funds are available to recipients until expended or returned to the U.S. Treasury.

The statute defines eligible revenue sharing counties to include any county, parish, or borough:

- That is independent of any other unit of local government; and
- That, as determined by the Secretary, is the principal provider of government services for the area within its jurisdiction; and
- For which, as determined by the Secretary, there is a negative revenue impact due to implementation of a federal program or changes to such program.

Chippewa County is eligible to receive $50,000 in 2022 and $50,000 in 2023. I have authorized the Finance Director to log into the Treasury Submission Portal and submit a request so we can receive our payments. After we receive the funds, we will need to submit periodic reports to the Treasury, similar to the ARPA reporting requirements.

I recommend that we utilize the funds to pay for an unexpected expense in the Sheriff's Department. The cost is for a juvenile that is being housed at the Eau Claire Detention Center. The cost per day is $225. If there are 31 days in the month, it costs us $6,975, for 30 days it is $6,750. The estimated cost for 2022 is $56,250. The estimated cost for all of 2023 is $82,125. My logic for recommending the funds be used for this purpose is that these funds were not anticipated and the expense was not anticipated.

We do not know how long the juvenile will be housed in Eau Claire County, but we do know, at this time, the next court hearing is scheduled for August of 2023. Therefore, we anticipate a significant unexpected expense to our Sheriff's Department budget.

I intend to provide this report to the Executive Committee at the October 18, 2022 meeting and to the County Board on November 8, 2022. If you have any questions or feel the funds should be utilized in a different manner, give me a call.

Randy Scholz
County Administrator

711 N. Bridge Street, Room 106
Chippewa Falls, WI 54729
rscholz@co.chippewa.wi.us
Ph: (715)
Fx: (715)

STATEMENT OF EXPLANATION
UPDATE ON CHIPPEWA COUNTY VIDEO PROJECT WITH CGI DIGITAL

October 26, 2022

TO: County Board Supervisors

FR: Randy Scholz

RE: County Video Project with CGI Digital

At the October 18, 2022, Executive Committee meeting, Charlie Walker and I gave an update on the County video project with CGI Digital. There was some confusion on what exactly the videos will showcase and the goal of this project. Several years ago, when I was with Lincoln County, we completed a similar initiative and I thought it may help to provide a link to those videos so you all have a better understanding.

Lincoln County videos
https://www.elocallink.tv/m/v/player.php?pid=w9aNQz74&fp=wilincco18_welr_iwd#c|wilincco18_cocr_iwd
<https://www.elocallink.tv/m/v/player.php?pid=w9aNQz74&fp=wilincco18_welr_iwd>

Thanks,
Randy Scholz

History:
10/18/22 Executive Committee REVIEWED

Department of Administration

Randy B. Scholz, County Administrator

October 11, 2022

TO: Executive Committee

FR: Randy Scholz & Charlie Walker

RE: Update on Chippewa County Video Project with CGI Digital

Digital advertising targeting people looking for homes, jobs or tourist attractions in Chippewa County continues to grow. Chippewa County residents and businesses continue to build a foundation of what "a great community" is! Built on the ingredients of entrepreneurship, affordability, wholesomeness, proximity, safety, and fiscal responsibilities, Chippewa County has embarked on a program that will provide video messages we can post on our website https://www.co.chippewa.wi.us.

In March 2022, the County was approached by CGI Digital to work in partnership to assist Chippewa County with web site video enhancements. By partnering with CGI Digital in their community video program, it gives Chippewa County the opportunity to showcase what makes us special while attracting new residents, tourists, businesses, and entrepreneurs. With jobs unfilled and young people moving away, many counties are ahead of Chippewa County and are doubling down on efforts to attract new citizens. This program will be a step towards marketing Chippewa County to potential new citizens.

The Program will at no cost to Chippewa County:

- Produce 4 video chapters with subject matter that includes, but is not limited to: Welcome, Healthy Living, Economic Development/Jobs.
- Provide CGI's patented OneClick™ Technology and encode all videos into multiple streaming digital formats to play on all computer systems, browsers, and Internet connection speeds; recognized player formats include WindowsMedia™ and QuickTime™.
- Store and stream all videos on CGI's dedicated server.
- Afford businesses the opportunity to purchase various digital media products and services from CGI Digital and its affiliates.
- CGI Digital is solely responsible for sponsorship fulfillment including all related aspects of marketing, production, printing, and distribution.
- CGI Digital will assume all costs for the County Video Program.

The CGI Program will begin their business outreach in the next three quarters and is currently finalizing first drafts of video scripts. Video shoots are anticipated to occurred in the spring of 2023.

711 N. Bridge Street, Room 106
Chippewa Falls, WI 54729
rscholz@co.chippewa.wi.us
Ph: (715) 7
Fx: (715) 7

STATEMENT OF EXPLANATION

Resolution No. 56 - 22

RES. 56-22: RESOLUTION TO APPROVE CHIPPEWA COUNTY TAX LEVY TO BE COLLECTED IN 2023 - RANDY SCHOLZ

This resolution is bought pursuant to § 70.62, Wis. Stats., to approve the tax levy for 2023 for Chippewa County's operations. This resolution is required to be passed on an annual basis to establish the county's tax levy for the following year's budget.

Resolution No. 56 - 22

RES. 56-22: RESOLUTION TO APPROVE CHIPPEWA COUNTY TAX LEVY TO BE COLLECTED IN 2023 - RANDY SCHOLZ

WHEREAS, the Chippewa County Administrator has presented the 2023 Budget to the Chippewa County Board of Supervisors; and

WHEREAS, the Chippewa County Board of Supervisors met in regular session on November 3, 2022, considered all matters before it and recommends the adoption of the following resolution for financing of the county operations for the year 2023;

NOW, THEREFORE BE IT RESOLVED, that the Chippewa County Board of Supervisors approves a levy against the taxable property in Chippewa County in the following amounts:

State Taxes for:

Forestry Mill Tax pursuant to Wis. Stats. § 70.58(2)		
Property Valuation		$0.00
State Forestry Tax Rate		X 0.000
		$0.00
Special Charges upon County for Charitable and Penal Purposes		
Cost of Proceedings - Charges		$0.00
Cost of Proceedings - Credits	-0.00	
		$0.00

County Taxes for:

General Fund	$13,703,013
Special Revenue Funds	$ 2,751,518
Internal Service Funds	$ 4,486,535
	$20,941,066.00

Town, Village and City Taxes for:

Town, Village and City Illegal Tax Certificate Charge back	
	$0.00

GRAND TOTAL ALL TAXES AND CHARGES **$20,941,066.00**

FINANCIAL IMPACT:

$20,941,066.00 of Tax Levy for 2023 Budget

11/8/2022	**County Board**
RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Robert Teuteberg, District 14
SECONDER:	Ronald McGill, District 16
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	James Flater, Matthew Peterson

Approved as to Form:

Todd A. Pauls
Todd A. Pauls, Corporation Counsel 10/24/2022

Lori Zwiefelhofer
Lori Zwiefelhofer, Finance Director 10/24/2022

Randy B. Scholz
Randy B. Scholz, County Administrator 10/24/2022

STATEMENT OF EXPLANATION

Resolution No. 57 - 22

RES. 57-22: RESOLUTION TO CREATE THE COMMUNITY WELL DRILLING PROJECT AD HOC COMMITTEE OF THE LAND CONSERVATION AND FOREST MANAGEMENT COMMITTEE - RANDY SCHOLZ AND LYNDA SCHWEIKERT

Passage of this resolution will create an ad hoc committee of the Land Conservation and Forest Management Committee. The committee will be known as the "Community Well Drilling Project Ad Hoc Committee" and its purpose will be to do the following:

1. Locate areas that would benefit from a community well to provide safe drinking water for those affected by high nitrates in the ground water.
2. Analyze existing permitted non-transient, non-community wells to see if those wells could be utilized as refill stations.
3. In the absence of existing wells, identify locations to drill community wells in priority areas that will have the highest success rate of producing safe drinking water.
4. Present the ad hoc committee's findings and recommendations to Land Conservation and Forest Management Committee.

It is anticipated that members of the ad hoc committee would include a groundwater education specialist, a hydrologist, a DNR water supply specialist, a Wisconsin Water Well Association representative, and representatives from effected towns. These members would be solicited and approved by the Land Conservation and Forest Management Committee. The meetings will be facilitated by the Director of the Land Conservation and Forest Management Department.

Resolution No. 57 - 22

RES. 57-22: RESOLUTION TO CREATE THE COMMUNITY WELL DRILLING PROJECT AD HOC COMMITTEE OF THE LAND CONSERVATION AND FOREST MANAGEMENT COMMITTEE - RANDY SCHOLZ AND LYNDA SCHWEIKERT

WHEREAS, certain areas of Chippewa County have high nitrate levels in the groundwater to such an extent that some residents in those areas are not able to drink the wellwater; and

WHEREAS, the Land Conservation and Forest Management (LCFM) Committee has determined that American Rescue Plan Act (ARPA) funds should be used to study, develop and implement a community well program for use by County citizens whose groundwater is affected by nitrates; and

WHEREAS, the LCFM committee has determined that an ad hoc committee of the LCFM Committee should be created with a membership of various groundwater experts and representatives from the towns affected to do the following:

-Locate areas in the County that would benefit from a community well to provide safe drinking water for those affected by high nitrates in the ground water.

-Analyze existing permitted non-transient, non-community wells to see if those wells could be utilized as refill stations.

-In the absence of existing wells, identify locations to drill community wells in priority areas that will have the highest success rate of producing safe drinking water.

-Present the committee's findings and recommendations to the LCFM Committee; and

WHEREAS, the membership of the ad hoc committee would be solicited and approved by the LCFM Committee; and

WHEREAS, it is anticipated that members of the ad hoc committee would include a groundwater education specialist, a hydrologist, a DNR water supply specialist, a Wisconsin Water Well Association representative, and representatives from affected towns; and

WHEREAS, the committee will be known as the "Community Well Drilling Project Ad Hoc Committee" and the meetings will be facilitated by the Director of the Land Conservation and Forest Management Department; and

WHEREAS, this ad hoc committee will hold meetings as needed to complete its mission;

NOW, THEREFORE BE IT RESOLVED, that the Land Conservation and Forest Management Committee hereby creates the Community Well Drilling Project Ad Hoc Committee to study, develop and recommend to the Land Conservation and Forest Management Committee how to implement a community well drilling project; and

BE IT FURTHER RESOLVED, that the membership of the Community Well Drilling Project Ad Hoc Committee shall include various groundwater experts such as a groundwater education specialist, a hydrologist, a DNR water supply specialist, and a Wisconsin Water Well Association representative, as well as representatives from towns in the County affected by nitrates in the groundwater; and

BE IT FURTHER RESOLVED, that the mission of the Community Well Drilling Project Ad Hoc Committee shall be on the following:

-Locating areas in the County that would benefit from a community well to provide safe drinking water for those affected by high nitrates in the ground water.

-Analyzing existing permitted non-transient, non-community wells to see if those wells could be utilized as refill stations.

-In the absence of existing wells, identifying locations to drill community wells in priority areas that will have the highest success rate of producing safe drinking water; and

BE IT FURTHER RESOLVED, that the Community Well Drilling Project Ad Hoc Committee shall present its findings and recommendations to the Land Conservation and Forest Management Committee and the County Board after completion of its mission.

Forwarded to the County Board by the Land Conservation and Forest Management Committee.

FINANCIAL IMPACT:

The fiscal impact by passage of this resolution would be limited to per diem and/or mileage payments to the members of the committee.

11/8/2022	**County Board**
RESULT:	**APPROVED AS AMENDED [UNANIMOUS]**
MOVER:	Jason Bergeron, District 7
SECONDER:	Joel Seidlitz, District 9
AYES:	Gullickson, Schmitt, Steele, Bischel, Sikorski, Bergeron, Ericksen, Seidlitz, Calkins, Bomar, Berg, Teuteberg, Eisenhuth, McGill, Rohmeyer, Hunt, Hull, Mueller, Ives
ABSENT:	James Flater, Matthew Peterson

History:

10/19/22 Land Conservation & Forest Management Committee FORWARD TO COUNTY BOARD

Approved as to Form:

Todd A. Pauls, Corporation Counsel 10/11/2022

Lori Zwiefelhofer, Finance Director 10/11/2022

Randy B. Scholz, County Administrator 10/11/2022

103

STATEMENT OF EXPLANATION
FACILITY USE POLICY REVISIONS - SECOND READING - LARRY RITZINGER

The County Board adopted the Facility Use Policy on March 8, 2022. The amendments to the Facility Use Policy consist of the following:

- The removal of all language that references the Chippewa County Firearms Range Use policy.
- Updates to the Courthouse hours of operation so that they accurately reflect the Human Resource Policy Manual.
- A small change by the Information Technology Division regarding availability of A/V - internet services in Conference Rooms.

History:
09/28/22 Facilities & Parks Committee FORWARD TO COUNTY BOARD
10/11/22 County Board FIRST READING

*** Proposed Revisions – Draft 9/16/22 ***

FACILITY USE POLICY

Purpose

Chippewa County facilities are primarily used for official county functions by elected officials and staff. This policy identifies the hours of operations to provide for a fully functioning Courthouse facility and governs the use of public areas within the Government Center Campus.

Definitions

The Government Center Campus includes parking lots A, B, C, D1, D2 and E, along with the courthouse, Sheriff's Department, Jail, 21 E. Spruce Street building, and the maintenance shop at 109 E. Spruce Street, Chippewa Falls.

The Highway Administration Building includes 801 E. Grand Avenue, Chippewa Falls.

Courthouse Hours of Operation

To provide for safety, security and energy efficiency the normal recognized hours of operation for the Chippewa County Courthouse per Ordinance Sec. 2-2 are ~~Monday – Friday, 8:00 a.m. – 4:30 p.m.~~7:30 a.m. to 4:30 p.m. Monday through Thursday and 7:30 a.m. to 11:30 a.m. on Friday; closed weekends and holidays. During the normal hours of operation, the Courthouse is fully functioning with all lights, HVAC, electrical and elevator systems activated. During after-hours and weekends the systems are de-activated and not fully functional. The Courthouse does provide for some limited evening hour activities for County Board and committee meetings, and incidental department business.

Primary Use of County Facilities

The primary use of county facilities is to conduct county government business. Consequently, groups that are a part of Chippewa County Government have sole use of most facility space and priority use of meeting rooms and other public facility space.

Access

Unlimited access to the Courthouse is available Monday – Friday, 7:30 a.m. – 5:00 p.m. After–hour entry is limited to the High Street Entrance #3 and Cedar Street Entrance #4. These doors will remain open Monday through Thursday until 6:00 p.m., unless evening meetings are scheduled, and Friday until 5:00 p.m.

- Meetings should not be scheduled before 7:45 a.m. to allow the attendees enough time to gain access to the facility and arrive to the meeting on time.

Priority Use for Public Areas

Priority for use shall be approved based on the type of use/activity as follows from highest to lowest priority:

1. The Chippewa County Board of Supervisors;
2. Formal and standing committees of the Board of Supervisors;
3. The County Administrator;
4. Boards and commissions appointed by the Board of Supervisors or the County Administrator;
5. County staff for purposes of county business;
6. Non-profit entities holding public meetings, or conducting official business related to a county service or program or public purpose activities.

If a scheduling conflict arises between the above groups, the higher priority user will have the reservation priority. Any conflicts will be resolved by the County Administrator.

Only non-profit citizen groups that are located in or do business in Chippewa County are permitted to use public areas in county facilities and county grounds to the extent permitted by law. Such use must not interfere with county government functions, operations and business.

The County reserves the right to implement a user fee for non-profit users if a user does not fully comply with this policy.

Attorneys, mediators and other court related personnel conducting court related functions have open access to the conference rooms identified as attorney conference rooms on the second floor of the Courthouse.

Security

To provide for the security and safety of visitors and staff, County/State personnel and other designated courthouse occupants are issued identification cards which must be worn at all times while in the courthouse. Please see the Identification and Access Card Policy for specific details.

Definition of Terms

A. Courthouse Public Use Areas

- Courthouse Grounds (West Lawn)
- Courthouse Parking Lot A (North)
- Courthouse Parking Lot D-1 (South)
- Courthouse Parking Lot E (West)
- Courthouse Cul-de-Sac Entrance #1
- Courthouse Room 001 – Small Assembly Room
- Courthouse Room 003 – Large Assembly Room
- Courthouse Room 005 – Lower Level Conference Room
- Courthouse Room 016 – Lower Level Conference Room
- Courthouse Room 119Q – First Floor Conference Room
- Courthouse Room 226 – Second Floor Conference Room
- Courthouse Room 227 – Second Floor Conference Room

***Note**: Other county facilities ~~including the Public Firearms Range~~ may have separate public use policies that govern public use of those facilities. Not all County facilities are open for public use. The Highway Department is not generally available for public use unless written approval is received from the Highway Commissioner.*

B. Non-profit entity

A non-profit entity is an agency, corporation, partnership or governmental entity, which can provide legal verification of either its non-profit status (including approved IRS non-profit status), or governmental relationship.

C. For-profit entity

A business or other organization whose primary goal is making money (a profit), as opposed to a nonprofit organization which focuses a goal such as helping the community and is concerned with money only as much as necessary to keep the organization operating.

D. Public purpose

An activity in which the action or direction concerns, affects, or is of benefit to the County or the greater County community, not just those affiliated with the group.

Terms of Use

The use of any county facility by profit-making groups or for profit-making purposes is generally prohibited. No business, non-profit, or personal organization shall be allowed to solicit business or sell items for profit without the prior permission of the Chippewa County Facilities & Parks Committee. This prohibition does not apply to those vendors approved to conduct business by the Department of Administration.

No alcoholic beverages shall be served, or consumed in county facilities listed in this policy. No person(s) impaired by alcohol shall be permitted in county facilities. For additional guidelines related to the Parks or County Forest Lands ~~and/or the Public Firearms Range~~ please reference County ordinance chapters 50 and 16 ~~and the Public Firearms Range webpage~~.

Smoking of tobacco products is prohibited in any enclosed building as provided by Wisconsin Statutes §101.123. In addition, the smoking of tobacco products and the use of smokeless tobacco products is prohibited in any enclosed building and/or on the grounds by Chippewa County Ordinance §48-92(b). For additional guidelines related to the Parks or County Forest Lands ~~and/or the Public Firearms Range~~ please reference County ordinance chapters 50 and 16 ~~and the Public Firearms Range webpage~~.

Weapons and firearms are prohibited in all county facilities unless possessed by licensed law enforcement professionals on official business. For additional guidelines related to the Parks or County Forest Lands ~~and/or the Public Firearms Range~~ please reference County ordinance chapters 50 and 16 ~~and the Public Firearms Range webpage~~.

Functions occurring in county facilities shall not violate any City of Chippewa Falls, Chippewa County, State of Wisconsin or federal applicable laws, ordinances or regulations.

There shall be no partisan political activities, political news conferences, or other events designed to announce or support any candidate for public office regardless of party or non-party affiliation in county

facilities. The County may allow current state representatives to hold listening sessions at the Courthouse if rooms are available.

Permission to use Chippewa County facilities shall not in any way constitute an endorsement by the County of the user group or individual, or their policies and activities and the County assumes no obligation or responsibility for the activities of the user group or individual.

Signs, emblems, banners, pennants, etc. may not be affixed to any building surfaces, steps, walls or light fixtures. User groups may post events on any of the approved bulletin boards, or cork strips available in the Courthouse hallways or meeting rooms by contacting the County Clerk's Office. In addition, users may affix notices no larger than 8½ x 11 inches to the approved sign stands that are located at each entrance and/or in the Cul-De-Sac Entrance #1 closet to direct meeting participants to proper meeting locations. Advertising items that are self-standing may be put into place before the scheduled start of the meeting or event, and must be removed at the conclusion of the meeting. In addition, display space may be available in the Courthouse Cul-de-Sac Entrance #1 for items that non-profit organizations desire to display to courthouse employees and the general public. Displays must fit on a standard folding table that will be provided for use by the County.

Equal Access

This policy shall apply to all groups and individuals that have requested use of the public areas of county facilities and grounds as defined in this policy. No group or individual shall be excluded from equal access to said grounds and facilities because of considerations of gender, race, sexual orientation, religious or political persuasions or views. However, use may be denied or terminated if there is a violation of the rules set forth in this policy and/or if the use poses health or safety risks.

Liability

Any non-Chippewa County Governmental group using the public use areas of county facilities as defined in this policy shall:

1. Be required to release the county from any liability for damages caused to the user or its property during the times of use.

2. Hold the county harmless from any liability to third parties for injury caused by the group or any persons or groups to attend the event.

3. Be liable to the county for any damages to county property or injuries to county employees or agents caused by the group or by a person attending the group's events, whether or not the damage is the result of negligence, intentional acts or accident.

The granting of permission to use county facility space does not obligate the county to furnish any applicant with any service or utilities, or to render any support regarding personnel, fixtures, equipment or supplies. The county may furnish such assistance as it, in its sole discretion, determines appropriate.

The county does not warrant that any county facility space, fixtures or equipment is fit for any purpose, and the county shall not be responsible in case of damage or injury to property or person or the loss of individual property which may arise out of, result from, or be in any manner connected with the use thereof.

It is the user entity's responsibility to ensure that adults properly supervise all children.

Indemnification and Liability Insurance

Non-Chippewa County Governmental groups understand and agree that using space, fixtures and equipment may expose user and others to risks. Such users voluntarily agree to assume all such risks, and to release and hold harmless Chippewa County and the county's supervisors, directors, officers, employees, volunteers and agents from and against any and all claims regarding damage to property or injuries to or death of any person(s), and to defend, indemnify and hold harmless Chippewa County and the county's supervisors, directors, officers, employees, volunteers and agents from any and all claims, demands, suits, actions or proceeding of any kind in nature, of or by anyone whatsoever, in any way resulting or arising out of activities, action or inactions of the user group. A representative of all non-Chippewa County Governmental groups shall sign an indemnification release (DOA-103-A) prior to reserving space.

Chippewa County reserves the right to require a public user of county facilities to provide adequate liability insurance prior to the use of county facilities.

Space Arrangement, Equipment, Food, Beverage, Fixtures and Utilities

Tables, chairs, fixtures and other equipment may not be removed from their assigned room without permission.

The Small Assembly Room (001) and Large Assembly Room (003) can be reconfigured to user specifications (see Process for Scheduling Facilities). At the conclusion of the permissible use, the user entity shall arrange the space back to the original configuration and condition.

User entities shall be responsible for any costs of repair or replacement incurred as a result of action or inaction by the user entity during approved use of the space.

No food and only covered beverages are allowed in the County Board Room (302). Food and beverages are allowed in all other courthouse conference rooms. Users shall discard all waste generated during the approved event.

Non-county organizations are prohibited from using the sound system in the Small Assembly Room (001) and Large Assembly Room (003). ~~The County shall provide Internet access to users of~~ Guest Wi-Fi is available for visitors to use in the conference room~~s. in the Small Assembly Room (001), Large Assembly Room (003), Room 016, and Room 119Q.~~

User entities or their representatives shall not adjust the heating or lighting.

Process for the Scheduling Facilities

A. Interior Space – Courthouse:

Non-county organizations should contact the County Clerk's Office to complete the Facility Use Application.

B. Exterior Space – Government Center Campus:

To schedule an outside parking lot, the courthouse grounds, or the internal Cul de Sac Entrance #1, contact the Facilities and Parks Division to complete the Facility Use Application, which will then be approved or denied.

~~C. Public Firearms Range:~~

~~1. To schedule use of the Public Firearms Range contact the Facilities & Parks Division to complete the Facility Use Application. The completed application should include the requested dates, start/end time, and the area requested to be used (Hand Gun Range, Long Gun Range, or Training Facility)~~

~~2. Tables and chairs are available for use, however the responsibility for setup and restoration rests solely with the user entity.~~

Cancellation of Permission and Right to Refuse Permission

In the event county government is declared closed due to inclement weather or other reasons, any permission to use the facility or grounds is automatically withdrawn during the closure period. In such an event, the county shall not provide notice of cancellation. Notices of Courthouse closure are generally announced through local radio broadcasts. Users shall be solely responsible for notifying event participants if a closure of the Courthouse or public use grounds occurs.

Notwithstanding the above closure notice, the county reserves the right to cancel, move or preempt scheduled use of a county facility and further reserves the right to access and enter the reserved space at any time. The county further reserves the right to refuse permission to use county facilities.

The County reserves the right to charge user for any costs incurred by County due to use or misuse of space, fixtures, and equipment. **User is expected to ensure space, fixtures, and equipment are left as they were found, in a clean, undamaged, presentable and organized manner.** In the event cleaning, repair or other actions are necessary due to the actions or inactions of user. User may be assessed reasonable costs, and barred from future use of any space at County Facility discretion, for violation of the written Facility Policy of any County Facility. User may not reserve or use any space unless user has paid all costs and amounts due regarding prior usage of any space.

Department of Administration
Human Resources Division

To: County Board Supervisors

From: Toni Hohlfelder, Human Resources Director

Date: October 11, 2022

Subject: Summary of the HR Policy Manual Recommended Changes

To assist in reviewing three HR Policy Manual changes we are bringing forward for approval, below are a few details about each minor change:

1. Section 1: Hours of Work – Due to the County Board approving the resolution to update the Courthouse Hours, the Hours of Work policy needs to be updated to align with this change.

2. Section 17: Overtime and Compensatory Time – The second policy change is due to an oversight with the addition of section 17(j) for non-exempt employees to have their compensatory time paid out annually.

   The suggested change is to section 17(e) to add another circumstance to pay out compensatory time when a non-exempt employee transfers to another non-exempt position. This will ensure that the pay out is at the correct hourly wage that the compensatory time was earned.

3. Section 62: Drug and Alcohol Testing – A minor error was identified under section 62(d) to the Blood Alcohol Content (BAC) listed in the policy. It should read .03999 vs. .3999.

If you have any questions or suggestions prior to the Executive or County Board meetings, please don't hesitate to email me at thohlfelder@co.chippewa.wi.us or call me at 715-726-7970.

PROPOSED REVISIONS

1. Hours of Work

a. Purpose

To provide employees with hours of operation and a policy to assist Department Heads, managers and employees in creating ~~regular work hours and~~ work schedules that ~~while~~ ensur~~esing staffing coverage necessary~~ proper office coverage for effective operations. ~~Hours of work and~~ W~~w~~ork schedules shall generally be approved ~~determined~~ by the Department Head and in some cases shall be approved by the County Administrator.

b. Hours of Operation~~Business Hours~~

Note: The Hours of Operation are established by County ordinance Sec. 2-2.

~~Chippewa County~~All offices in the c~~C~~ourthouse ~~office hours~~ are generally staffed and open to the public from 7~~8~~:~~03~~0 a.m. to 4:30 p.m. Monday through Thursday and 7:30 a.m. to 11:30 a.m. on Friday except for established holidays as determined by the County Board.

All offices in the Law Enforcement Center are generally staffed and open to the public from 7:30 a.m. to 4:30 p.m. Monday through Thursday and 7:30 a.m. to 11:30 a.m. on Friday.

All offices at the ~~Chippewa County~~ Highway Department ~~hours~~ are generally staffed and open to the public from 6:00 a.m. to 4:00 p.m. Monday through Thursday from May to November or 6:30 a.m. to 4:30p.m. Monday through Thursday from November to May.

c. Schedule

The County reserves the right to schedule and/or change all hours and schedules of work as deemed necessary and nothing contained herein shall be construed as a guaranteed work week. The core hours of operation for County Courthouse offices are generally 7~~8~~:3~~0~~0 a.m. to 4:30 p.m. Monday through Thursday and 7:30 a.m. to 11:30 am on Friday. However, this does not guarantee a work schedule of such, and scheduling may be adjusted according to the operational needs of a department.

The core hours of operation for the Highway Department are generally 6:00 a.m. to 4:00 p.m. or 6:30 a.m. to 4:30 p.m. Monday to Thursday depending on the season, however this does not guarantee a work schedule of such, and scheduling may be adjusted according to the operational needs of a department.

Certain departments may work varied hours based on 24/7 operations, customer needs, including the Sheriff's Department.

d. Alternate Schedule

Alternate schedules are typically permanent schedules that deviate from the core hours of operation for the County. Examples include 8-hour shift schedules, 9-hour shift schedules, 10-hour shift schedules, 12-hour shift schedules, mixed shift schedules or schedules starting or ending earlier or later in the day than the core hours of operation detailed above under the Schedule section. Alternate schedules require the approval of the County Administrator. The Department Head may discontinue the alternate schedule and should provide advance notice of such change to affected employee(s) whenever possible.

e. Flexible Schedules

Flexible Schedules enhance the ability of the County to fulfill its responsibilities, render services to the public, and enhance employee morale. For purposes of this section, a flexible schedule is not a permanent schedule or shift change. Rather, a flexible schedule is designed to offer the employee and the Department Head flexibility to alter a shift as needed for a short term, temporary or one-time basis. A flexible schedule may be established upon request of the employee, with the prior approval of the Department Head or designee. The Department Head may discontinue or alter the flexible schedule. When discontinuing or altering an established flexible schedule, the Department Head will normally provide advance notice of such change whenever possible.

f. Workweek

The normal work week shall consist of seven consecutive calendar days, starting at 12:00 a.m. on Sunday and ending at 11:59 p.m. on the following Saturday of each calendar week for all departments.

g. Maximum Hours Worked

Employees may be required to work additional hours in a day to meet operational demands for a department. Employees are required to have at least eight (8) hours off after 16 consecutive hours worked.

1. Extended Operations Exceptions

Certain operations may require employees to work longer consecutive hours (such as snow removal or dispatch emergency communications). During extended operations, employees may request rest time to their Department Head/Manager. The Department Head is then required to make arrangements for such rest time on an individual basis, giving consideration to the needs of the employee as well as continued coverage for these services. The Department Head/Manager has the authority to require employees take rest time and remove them from work at any point while providing extended operations. Rest time shall not count as hours worked.

h. Work Performed Outside the County Workplace

Generally speaking, non-exempt employees shall perform their duties only at a County worksite. (Examples of an obvious exception to this are those positions which require employees to travel to clients' homes and other similarly situated positions.) Non-exempt employees shall receive advanced approval from their Department Head for any work performed outside the County workplace. Non-exempt (hourly) employees approved for work outside the County workplace shall document and submit their hours, including but not limited to any and all time spent accessing work related emails and other programs and files, according to the payroll policies.

i. Daylight Savings Time

Employees who are required to work during the change of Daylight Savings Time shall be paid for the hours actually worked.

j. Annual Hours

1. Full-Time Status

The normal workweek for regular full-time employees is generally 40 hours as designated by the County. The annual hours of full-time employees are normally 2080+ hours.

2. Part-Time Status

The workweek for any regular part-time employee shall be designated by Chippewa County and normally is scheduled between 20-28 hours/week. The annual hours of part-time employees ranges between 1040-1500 hours.

3. Limited-Term (Annual or Seasonal) Status

The workweek for any limited-term employee (LTE) shall be designated by Chippewa County. The annual hours of an LTE shall not exceed 975 hours without County Administrator approval. Approval may be granted for a temporary increase in hours, which is budget neutral and does not result in becoming WRS eligible. The normal schedule of an Annual LTE is variable and between 1-19 hours/week for the entire year. The normal schedule of a Seasonal LTE is up to 40 hours/week and by the very definition, shall be seasonal. If the Seasonal LTE returns the following season, there should be a 6 month break in service. In rare circumstances, with Human Resources Division approval, a minimum of a 13 week break in service may occur.

(Section 1 amended by the County Board 05/14/13; 12/10/13; 12/09/14; 12/08/15; 03/13/18; 11/6/18; 11/10/2020; 09/13/2022)

PROPOSED REVISIONS

17. Overtime and Compensatory Time

a. Purpose

To provide a consistent system for distributing overtime in compliance with the overtime-pay provisions of the Fair Labor Standards Act (FLSA).

b. Definitions

Each position is designated as either "Non-exempt" or "Exempt" from the federal Fair Labor Standards Act and state wage and hour laws. Employees should contact the Human Resources Division if they are unsure of their position's designation.

1. Non-Exempt positions that are paid on an hourly basis and are entitled to overtime pay for hours worked in excess of 40 hours per week, excluding premium overtime pay (29 C.F.R. §778.201).

2. Exempt positions that are generally paid on a salary basis and are excluded from specific provisions of federal and state wage and hour laws and are not eligible for overtime pay.

c. Overtime

Non-exempt employees may receive pay for overtime hours. This shall be paid at time and one half the hourly rate of pay for any hours worked in excess of 40 hours per workweek.

1. Facilities and Parks Division Exception

Non-exempt Facilities and Parks employees shall receive overtime at a rate of time and one-half their regular hourly rate for all hours worked for winter maintenance between the hours of 6:00 p.m. – 6:00 a.m., unless normally scheduled, and for hours worked for winter maintenance on Saturdays and Sundays.

Non-exempt Facilities and Parks employees shall receive overtime pay at time and one-half their regular hourly rate for time worked outside of their normal work schedule/shift for emergency situations. A minimum of two (2) hours shall be paid except for those hours that are part of the normal work schedule/shift. Management shall have the discretion to determine the workday thereafter. Emergency situation examples include weather-related damage, facility damage, and flooding, but excludes snow/ice removal and construction projects.

Overtime hours worked under this section is considered premium overtime pay and shall not be calculated in the regular rate of pay for the purposes of calculating FLSA overtime (29 C.F.R §778.203 and §778.204 or as amended).

2. Sheriff's Department Management Exception

Sheriff's Department Management who are exempt may be paid overtime at their straight hourly rate for hours in excess of forty (40) in any one (1) workweek for special events in which all operating costs, salaries, and fringes are billed back to the event organizer for reimbursement. Such events do not include normal duties and responsibilities of the job (i.e. reporting to the scene of an accident after normal work hours). Events covered include large assembly events and music events.

3. Sheriff's Department Exception

Chippewa County has established an alternate work period for Jailers, Jail Sergeants and Patrol Sergeants working 12-hour shifts. If the Jailer, Jail Sergeant or Patrol Sergeant is assigned the alternate work period, the following exception applies. As allowed under Section 7(k) of the Fair Labor Standards Act (FLSA), the alternate work periods for Jailers, Jail Sergeants and Patrol Sergeants rotates on a 14-day work period basis. The work period for Jailers, Jail Sergeants and Patrol Sergeants shall consist of fourteen (14) consecutive calendar days starting at 12:00 a.m. on Sunday and ending at 11:59 p.m. on Saturday 14 days later. The overtime threshold within this work period shall be 84.0 hours for purposes of hours worked. Calculation of overtime and/or compensatory time shall be based on hours of work in excess of 84.0 hours per 14-day work period for the purposes of this Policy. In instances when a Jailer, Jail Sergeant or Patrol Sergeant uses PTO or Compensatory Time during one week of the 14-day work period, the employee shall earn OT after the scheduled hours for that week (36 hours or 48 hours) only in the week in which the PTO or Compensatory Time were not used, as long as there are no unpaid normally schedule hours during the 14-day work period.

4. Highway Department Exception

Non-exempt Highway employees shall receive overtime at a rate of time and one-half their regular hourly rate for hours worked outside of their normal work day/shift. All hours worked in excess of, or outside of, the normal work day/shift shall be approved by the Highway Commissioner or designee. A minimum of two (2) hours shall be paid if an employee is called into work, except for those hours that are part of the normal work day/shift that precede or immediately follow the shift.

Overtime hours worked under this section is considered premium overtime pay and shall not be calculated in the regular rate of pay for the purposes of calculating FLSA overtime (29 C.F.R §778.203 and §778.204 or as amended).

d. Compensatory Time

1. Exempt

It is understood that Department Heads, Managers, and other exempt positions (as classified by your job description) are paid a salary for their overall responsibility and accountability and may work in excess of the normal work week in order to complete necessary job tasks. At the discretion of the

Department Head, (and County Administrator in cases of Department Heads) exempt employees who work in excess of 40 hours in a workweek (including Holiday pay) may qualify for compensatory time. Compensatory time shall be earned prior to use, is earned at straight time (hour for hour), and shall be tracked accordingly on the timesheet. Compensatory time balances for exempt non-management positions in the Criminal Justice Services, Public Health and Human Services Departments shall not exceed 40.0 hours. All other exempt employees shall not exceed 80.0 hours.

2. Non-Exempt

Non-exempt employees may receive overtime in the form of compensatory time (earned at time and one half) or paid time at one and one-half times their rate of pay for hours worked in excess of 40 in a workweek (excludes hours paid, such as workers' compensation, PTO, jury duty and/or compensatory time taken) at the employer's discretion. "Non-exempt" status is determined by the employer on a job-by-job basis. Compensatory time shall be tracked on the timesheet. Compensatory time balances shall not exceed 40.0 hours for all non-exempt positions (80.0 hours for non-exempt management positions). Once the maximum accrual amount has been met, employees shall be paid for any time worked in excess of 40 in a workweek at a rate of time and one-half.

a). Section 7(O) of the FLSA allows public sector employers to provide certain nonexempt employees with an option of whether to receive cash overtime or compensatory time earned at time and one-half. Department heads shall determine employee eligibility for earning compensatory time.

b). Non-exempt highway employees are not eligible for compensatory time and shall receive overtime in the form of pay only.

3. Increments of Time

Employees shall use Compensatory Time in increments of fifteen (15) minutes.

e. Compensatory Time Payout

All accrued and unused compensatory time shall be paid out for the following reasons:

1. If an employee changes positions that results in an exempt or non-exempt status change; or

2. If an employee transfers to another department; or

3. If an employee becomes an elected official for the County; or

4. If a non-exempt employee transfers to a new non-exempt position and there is also a pay change, the employee's Compensatory Time shall be paid out at the time of the transfer at the rate of pay prior to the transfer; or

45. When an employee separates employment from Chippewa County. A separation is defined as follows:

a). resignation or retirement from employment with Chippewa County

b). permanent layoff from employment

c). discharge from employment with Chippewa County

Compensatory time payout due to a change in position that results in an exempt or non-exempt status change, transfer to another department, or when an employee becomes an elected official shall be added to the payroll on the last day worked in the former position, paid at the regular rate of pay, to be paid in cash via the employee paycheck. The compensatory time paid shall not be considered time worked.

Compensatory time payout due to separation of employment shall be paid in accordance with Chippewa County's Separation from Employment Policy.

f. Approval

All overtime/compensatory time earned shall be approved in advance by the Department Head. If advanced approval is not obtained, the employee is not authorized to work the overtime. The Department Head has the sole right to approve or deny overtime and compensatory time requests. Failure to obtain prior approval may result in disciplinary action, up to and including discharge.

Requests to trade shifts cannot result in creating overtime/compensatory time for either party.

g. Compensatory Time Off

Use of compensatory time shall be requested by the employee as far in advance as reasonably possible, and shall be approved in advance by the Department Head. Employees shall follow written departmental procedures for requesting to take compensatory time. Requests to use compensatory time may be denied based on the needs and workload of the department or if other employees are already scheduled for time off. The Department Head has full authority to approve or deny said request.

h. Department Scheduling Procedures

Each department shall establish written procedures to ensure that compensatory time off requests are processed in a fair and equitable manner, with first consideration to be given to the efficient operation of the department. All departments shall file a copy of their updated written time off procedures with the Human Resources Division.

i. Accrual

Employees are not able to earn compensatory time or paid overtime (earned at straight time or time and one half) as a result of the use of paid leaves. No paid leave time shall be counted as hours worked for overtime purposes, including PTO, workers' compensation, jury duty, and compensatory time taken.

j. Non-Exempt Employee Annual Payout of Compensatory Time

Non-exempt employees shall be paid-out, at straight time, any unused Compensatory Time earned each calendar year on the last paycheck of the year it was earned. All non-exempt employees shall start every new year with a zero balance in their Compensatory Time accrual bank.

k. Safe Harbor

It is the policy of Chippewa County to comply with the salary basis requirements of the FLSA. Therefore, improper deductions from the salaries of exempt employees are prohibited. If it is felt that an improper deduction has been made to your salary, you should immediately report this to the Human Resources Director. Reports of improper deductions shall be promptly investigated and reimbursements provided if it is determined improper deductions occurred.

29 C.F.R 541.710 outlines the principles of public accountability in which public agencies and elected officials are held to a higher level of responsibility under the public trust which demands effective and efficient use of public funds in order to serve the public interest including the view that public employees should not be paid for time they do not work excluding the use of paid time as outlined in Chippewa County policy.

(Section 17 amended by the County Board 05/14/13; 12/09/14; 12/08/15, 03/13/18, 11/6/18; 11/10/2020)

PROPOSED REVISIONS

62. Drug and Alcohol Testing

a. Purpose

The County has a vital interest in maintaining a safe, healthy, and productive working environment for its employees. Chippewa County employees are prohibited from possessing, distributing, selling, or working under the influence of drugs or alcohol, which can be a serious safety risk to themselves, to other employees, or to the general public.

The Department of Transportation (DOT) and the Federal Highway Administration (FHWA) issued Federal Regulations (49 CFR Parts 40 and 382) implementing provisions of the federal Omnibus Transportation Employee Testing Act of 1991 which requires alcohol and controlled substance testing of drivers who are required to have a commercial driver's license (CDL) and details testing procedures for employees in safety-sensitive positions.

In order to further the County's goal of maintaining a drug and alcohol free workplace, the County has implemented a drug and alcohol testing policy. County positions that require a CDL or are classified as a safety-sensitive position require specific forms of drug and alcohol testing. All County employees may be subject to testing based on a reasonable suspicion of use.

b. Testing Requirements Defined

To assist the County in preventing employees from using illegal drugs, alcohol and controlled substances at all County work sites, drug and alcohol testing shall be administered under the following conditions:

1. Pre-Employment

a). The following position applicants are subject to Pre-Employment drug and alcohol testing as outlined in the job description:

1. All positions that are required to hold and maintain a valid Commercial Driver's License (CDL).

2. All Sherriff Department positions that are in "safety-sensitive" positions as defined under DOT Rule 49 CFR Part 40.

b). Applicants for employment subject to Pre-Employment testing shall be notified orally of the County's policy requiring Pre-Employment testing and the offer of employment shall be contingent upon the applicant submitting to a drug and alcohol test. The County shall deny employment to any applicant who tests positive for illegal drugs or a Blood Alcohol Content (BAC) result of .02 BAC or higher.

c). The County shall presume a positive test result if an applicant refuses to be tested.

2. Reasonable Suspicion

a). All employees shall be required to undergo a drug and/or alcohol test if the County has reason to believe the employee is using drugs or is under the influence of or impaired by alcohol.

b). If an employee suspects that another employee at work is under the influence of drugs and/or alcohol, the employee shall notify their supervisor or the Human Resources Division immediately.

c). When possible, the reasonable suspicion circumstance should be witnessed by two (2) or more supervisors who have received training in the detection of probable drug or alcohol use through observations.

d). The reasonable suspicion determination shall be documented by using the Reasonable Suspicion Check List Form located on the Employee Portal and submitted to the Human Resources Division immediately.

e). Indicators that an employee may be under the influence of drugs and/or alcohol include, but are not limited to:

1. Direct observation of physical symptoms or use.
2. The smell of drugs or alcohol on breath or person.
3. Evident physical impairment such as slurred speech or lack of coordination.
4. Information deemed reliable by the County from a source deemed credible by the County.
5. Conviction for the use, possession, or purchase of illegal drugs.
6. An excessive number of unexplained absences or tardiness.
7. A sudden or uncharacteristic and unexplained decline in productivity or performance.

f). If reasonable suspicion exists and a decision is made to require testing, the Human Resources Division shall notify the collection site that an employee is being escorted to the site for Reasonable Suspicion testing.

g). The employee required to undergo a Reasonable Suspicion test shall be driven, or escorted to the collection site by the employee's direct supervisor and (if possible) another supervisor or manager. The employee shall not be allowed to return to work until the results of the drug and/or alcohol test are received. Upon completion of the drug and/or alcohol test, arrangements shall be made for a spouse, family member, or friend to safely drive or escort the employee home. If none are available, the supervisor shall arrange for a taxicab to transport the employee to his or her home at the employee's expense. If the employee rejects the alternatives, the supervisor shall take measures as deemed appropriate to prohibit the employee from driving his or herself home.

h). An employee shall submit to testing when requested to do so by the County. The County shall presume a positive test result if an employee refuses to be tested upon reasonable suspicion.

i). Chippewa County managers shall be trained on Reasonable Suspicion indicators/standards every two (2) years and training shall be coordinated by the Human Resources Division.

3. Post-Accident

Post-Accident drug and alcohol testing shall be required only for accidents involving commercial motor vehicles as defined in this section.

a). CDL drivers and Sheriff's Department employees that are in "safety-sensitive" positions as defined under DOT Rule 49 CFR Part 40 shall be required to undergo Post-Accident drug and alcohol testing following an occurrence involving a commercial motor vehicle operating on a public road in commerce if any of the following occur, as defined in the Table below:

Table for §382.303(a) and (b)

Type of accident involved	Citation issued to the CMV driver	Test shall be performed by employer
i. Human fatality	YES NO	YES YES
ii. Bodily injury with immediate medical treatment away from the scene	YES NO	YES NO
iii. Disabling damage to any motor vehicle requiring tow away	YES NO	YES NO

b). Post-Accident drug and alcohol testing after an accident involving a commercial motor vehicle which requires that a urine drug specimen shall be collected (as defined above), shall be done so within thirty-two (32) hours of the accident. If a specimen cannot be collected in thirty-two (32) hours, the reasons and all attempts made shall be documented and submitted to the Human Resources Division.

c). Post-Accident drug and alcohol testing after an accident involving a commercial motor vehicle which requires that a breath alcohol specimen shall be collected (as defined above), shall be done so within eight (8) hours of the accident. If the specimen cannot be collected within the first two (2) hours, the reasons and all attempts made shall be documented and submitted to the Human Resources Division. Attempts shall be made to collect the specimen within the proceeding six (6) hours. If the specimen cannot be collected within the proceeding six (6) hours, the reasons and all attempts made shall be documented and submitted to the Human Resources Division. No further attempts may be made to obtain the specimen.

d). If the employee requires medical attention, necessary medical attention shall not be delayed in order to collect the required specimen(s).

e). Employees required to undergo a Post-Accident test shall be allowed to return to work prior to the County receiving results, if the County is satisfied that the employee does not present an immediate danger to

themselves or others. If the County is not satisfied that the employee does not pose an immediate danger to themselves or others, the employee shall not be allowed to return to work until test results are received by the County.

f). An employee shall submit to testing when requested to do so by the County. The County shall presume a positive test result if an employee refuses to be tested as required under Post-Accident.

4. Random

a). All employees that are required to hold and maintain a valid Commercial Driver's License (CDL) shall be subject to Random drug and/or alcohol testing. Quarterly, the County conducts unannounced drug and/or alcohol testing on a random selection of its CDL holders in compliance with the Federal Motor Carrier Safety Administration (FMCSA) guidelines.

b). Upon notification of his or her selection for Random drug and/or alcohol testing, the employee shall proceed to the collection site immediately. The employee shall report back to their scheduled work area after completion of the drug and/or alcohol testing.

c). All time spent driving to, during and from the Random test shall be recorded as work time.

c. <u>Collection Procedures</u>

1. A medical center designated by the County shall collect the sample(s) for testing utilizing the chain of custody procedures protecting the sample(s) identity. The County shall designate the laboratory that shall conduct testing. All testing shall be at the County's expense.

2. When an applicant or employee is required to submit to a drug and/or alcohol test, the individual shall be instructed when and where to report for the specimen to be collected. The applicant or employee shall be required to bring and present valid picture identification.

3. Urine samples shall be collected and used for drug testing. Urine samples shall be given in private, unless there is reason to believe that the individual has altered or substituted samples. In such circumstances, the individual may be required to give a second sample under direct supervision by a representative from the drug testing facility.

4. Breath samples may be used for alcohol testing.

5. Employees who are required to undergo a Reasonable Suspicion or Post-Accident test during their normally scheduled work hours shall use accrued Paid Time Off (PTO) for all time associated with the test if the results are positive. If the employee does not have PTO, the time shall be unpaid. If the test results are negative, all time associated with the testing that occurs during the normally scheduled work hours shall be considered work time and paid by the County.

6. If an employee refuses to submit to any required drug and/or alcohol test, the County shall presume a positive test result and the employee shall be subject to disciplinary action up to and including discharge.

d. Test Results and Employment Status

1. The results of the drug and/or alcohol testing shall be sent directly to the Human Resources Division.

2. The County shall deny employment to any applicant who tests positive for illegal drugs and/or a breathe alcohol test result of .02 BAC or higher.

3. All employees with a confirmed positive illegal drug test shall be discharged from employment.

4. All employees with a confirmed breathe alcohol tests where the Blood Alcohol Content (BAC) result is .02 BAC to .039999 BAC, may not return to work for 24 hours post results. The employee may also be subject to disciplinary action, up to and including discharge.

5. All employees with a confirmed breathe alcohol tests where the Blood Alcohol Content (BAC) result is .04 BAC or higher, shall be discharged from employment.

6. All employees testing positive for drugs or alcohol shall be advised of the available resources for evaluation and treatment including the names, addresses, and telephone numbers of Substance Abuse Programs, counseling and/or treatment programs. An employee who is discharged from employment due to a positive drug or alcohol test, may be reconsidered for employment, if there is a vacancy, upon successful completion of Substance Abuse Program, a mutually agreed upon number of negative drug and alcohol test results and a mutually agreed upon timeframe.

7. In the event any sample taken is found to be invalid or unreliable due to circumstances unrelated to the conduct of the employee or applicant, the employee or applicant may be required to provide a new sample for testing at the expense of the County.

8. In the event any sample taken is found to be invalid or unreliable due to circumstances related to the employee or applicant's conduct, the employee may be disciplined up to and including discharge or the applicant shall be denied employment.

e. Confidentiality

All test-related information, including the results of the drug and/or alcohol test, shall be treated as confidential information.

(Section 62 adopted by the County Board 1/8/19)

Department of Administration
Human Resources Division

To: County Board Supervisors

From: Toni Hohlfelder, Human Resources Director

Date: September 20, 2022

Subject: New Policies related to HIPAA

The purpose of this memo is to assist the County Board in reviewing several policies coming forward from the Department of Administration. The memo summarizes both the effort and history we have put into bringing these to the County Board for approval and a short summary for each of the policies.

History:

2015 Three Pillars (a consulting firm) performed a Risk Assessment as it relates to HIPAA for Chippewa County. The state of Washington had a lawsuit that involved a HIPAA breach where the company did not perform a risk assessment and the courts stated it was considered "gross negligence" by the organization when they had a serious breach occur.

2016 Upon completing the Risk Assessment, a HIPAA Workgroup was created and led by Holly Schlenvogt (now of HRT-Consulting) and included several members of DOA's IT Division, Jim Sherman, Corporation Counsel and a member of the fiscal teams in Human Services and Public Health who attended monthly meetings together. The goal of the workgroup was to correct the deficiencies identified in the risk assessment, create new procedures, forms, update current policies and add new policies related to HIPAA.

10/18/2017 I was invited to a HIPAA workgroup meeting to answer questions about a policy in our HR Policy manual and shortly after, I was asked to join the workgroup permanently due to my policy development experience.

1/22/2018 I officially joined the HIPAA workgroup and it was determined that Jim Sherman would be the Security Officer and I would be the Privacy Officer for Chippewa County. Since that time, we have had several potential privacy issues that I have followed and used all draft policies, procedures and forms to address and assist the County with.

12/10/2019 The IT Policy Manual was adopted by the County Board and includes three policies developed by this workgroup.

Feb 2020 Six additional polices were finalized and DOA was meeting to determine how to bring the new HIPAA polices forward and where they would be housed. We also needed to clarify which policies applied to all employees and which policies applied to the Workgroup or managers only. Then COVID hit, so this project was no longer prioritized. The HIPAA workgroup only met 4-5 times in 2020.

711 N. Bridge Street, Room 100
Chippewa Falls, WI 54729
HumanResources@co.chippewa.wi.us
Ph: (715) 726-7969
Fx: (715) 726-4585

2021 The workgroup started to meet more regularly (met 9 times in 2021) and was able to create several more policies drafts. Due to COVID, ARPA, the Board restructure and several other higher priority items, the HIPAA polices were tabled to bring at a later time.

2022 We now have updates to the currently approved ID and Access Policy and IT Policy Manual. We also have 4 new IT Policies, 5 new HIPAA polices and 2 new Facility & Parks Policies.

2023 - ? We will have additional polices to bring the County Board for approval in 2023: Auditing (HIPAA), Facility Maintenance (F&P), Technical Access Control (IT), System Build/Change Control (IT), Group Health (HR), Continuity of Operations (COOPS) and Continuity of Government (COGs).

In addition, Andy Bauer and I will create HIPAA training videos to ensure that all required employees and managers are properly and consistently trained on HIPAA related topics.

Lastly, the goal in 2023 is to perform another Risk Assessment to evaluate if we still have deficiencies from the original assessment performed in 2015. The workgroup will assist in addressing any issues that result from the assessment. We believe the workgroup can be disbanded at that time, as all policies, procedures and forms will be in practice.

SUMMARY OF THE POLICIES

HR Policy:

1. ID and Access Policy – revisions recommended
    a. A primary term that the consultant recommends the County changes from is Authorized Personnel changed to Authorized Workgroup members. HIPAA applies not only to Chippewa County personnel, but also interns, volunteers, contractors, business associates, etc.
    b. Replacement of County Electronic Access section was added and similar to the Replacement of ID Cards.
    c. All other recommended changes are from the HIPAA consultant to document in policy how we protect HIPAA information related to our IDs and Access.

IT Policies:

1. IT Policy Manual – revisions recommended
    a. Updated the Technology and Information Privacy and Security Policy only.
    b. Added a section regarding pagers and overhead paging.

2. Data backup Media Management – new
    a. The policy documents the County's current practice in backing up data and media in a policy.
    b. The policy documents what we will back up, the length of time it is required and how it is done.

3. Malicious Software Policy – new
    a. The policy defines what malicious software is and how the County has safeguards in place to prevent vulnerabilities from being exploited.

4. Remote Access Policy – new
    a. The County permits authorized Workforce Members to use remote access to access the network from home or another approved location.

711 N. Bridge Street, Room 100
Chippewa Falls, WI 54729
HumanResources@co.chippewa.wi.us
Ph: (715) 726-7969
Fx: (715) 726-4585

   b. The policy defines the types of remote access permitted and requirements for Workforce Members associated with using remote access

5. System Access Policy – new
   a. The policy documents the County's guidelines for Workforce Members on access to Electronic Protected Health Information (ePHI).
   b. It documents the policy on setting up, modifying and terminating access as well as requirements related to logging off and passwords.

HIPAA Polices (to be saved under DOA):

1. Business Associate Policy – new
   a. The policy documents the County's requirements for having a business agreement with vendors and the specific requirements in the agreements.
   b. The County's Corporation Counsel Division currently has a County Approval Procedure and this process will continue to be used in conjunction with this additional policy.

2. Contingency Plan Policy – new
   a. The policy is the first step in outlining the County's policy to have systems and plans in place to secure PHI, confidential information and other information in the case of an interruption in business caused by disaster or any emergency of any kind.
   b. Other policies, procedures and/or forms will include COOPS and COGS

3. Disposal of Confidential Information Policy – new
   a. The County has PHI, ePHI and other sensitive information that is required to be disposed of properly. This policy outlines the requirements.

4. Incidents Policy – new
   a. If there is a report of a possible HIPAA breach, this policy provides the requirements that the County will follow to investigate and if detected, contain and response appropriately.
   b. This draft policy has been being followed and the associated forms, check lists and tools provide by the Consultant related to this policy have been used since 2018 to assist the County in properly handling these situations.

5. Information Security Risk Management Policy - new
   a. The policy documents that the County will conduct risk assessments regularly to determine potential threats and vulnerabilities.
   b. The policy also documents strategies to mitigate the risks that may be identified in the assessment.
   c. Policy requires we complete a Risk Assessment every 4 years, but recommended every 2 years.

F&P Policies (going the Facilities & Parks Committee):

1. Facility Access and Physical Security Policy – new
   a. A policy that outlines how Chippewa County controls physical access into buildings.
   b. It also documents how we protect HIPAA information and provides details related to restricted vs unrestricted areas, doors, servers and data wiring and other facility safeguards

2. Key Issuance and Request Policy – new
   a. A policy that documents how we issue keys to new Workforce Members
   b. The policy also documents how we handle keys being returned upon separation or exiting.

711 N. Bridge Street, Room 100
Chippewa Falls, WI 54729
HumanResources@co.chippewa.wi.us
Ph: (715) 726-7969
Fx: (715) 726-4585

** Proposed Revisions **

IDENTIFICATION AND ACCESS POLICY

Purpose

The purpose of this policy is to establish a system that provides constant and immediate identification of Chippewa County Authorized ~~Personnel~~Workforce members to customers, clients, residents, visitors and other employees and maintain security of Chippewa County facilities, and enhance the personal security of Chippewa County Authorized ~~Personnel~~Workforce members, by identifying Authorized ~~Personnel~~Workforce members at Chippewa County work sites and residential or commercial properties served by the county while providing measured protection against unauthorized personnel from entering designated Secure Areas (including Restricted Areas). The system is effective only if there is active cooperation and compliance by all Authorized ~~Personnel~~Workforce members at all times. Any lenience in compliance and enforcement subjects the entire system to failure.

Scope

This Policy shall apply to all Authorized ~~Personnel~~Workforce members.

Definitions

1. Authorized ~~Personnel~~Workforce members include all county employees, elected officials and County Board Supervisors; student interns; non-uniformed state or federal employees with office space located within a county facility; designated individuals providing volunteer or contracted services on an on-going basis and who may have office space located within a County facility.

2. Project or Construction Contractors includes non-county employees who require temporary access to the facility to provide a specific service including, but not limited to service repair, emergency maintenance, construction, etc.

3. ID Card is a hard, plastic card used to identify Authorized ~~Personnel~~Workforce members for Chippewa County. The face of the card reflects the County name, an accurate photograph of the Authorized ~~Personnel~~Workforce member and the Authorized ~~Personnel~~Workforce member's name. ID Cards are color coded based on the Authorized ~~Personnel~~Workforce member's classification; for example, Chippewa County employee, intern, state employee, Housing Authority, contracted service, County Board Supervisor, etc.

4. Secure Area is an area within a County facility which access is controlled and the general public or clients are normally not permitted to enter freely. Also refer to the definition of a Restricted Area in the HIPAA Privacy and Security Definitions form located on the Employee Portal under Policies.

5. Access is the level of permission an Authorized ~~Personnel~~Workforce member is granted to enter specified locations within the Chippewa County courthouse.

6. Electronic Access Device is a small security hardware device with built-in authentication used to control or secure access to the building. The Electronic Access Device will have external and

internal access programmed into it and is typically stored on a key chain. Some Electronic Access Devices may be programmed to allow Authorized ~~Personnel~~Workforce members access to designated Chippewa County facilities outside of normal business hours or service areas during normal business hours.

7. For capitalized terms, refer to the HIPAA Privacy and Security Definitions form located on the Employee Portal under Policies / Department of Administration.

Policy

For the safety and security of the public, Chippewa County employees and facilities, all Authorized ~~Personnel~~Workforce members shall be assigned, and are required to display their County issued ID Card at all times while on County property, or while on duty and engaging in County business at a location, which is not County property as outlined below. Failure to wear the ID Card may result in disciplinary action up to and including termination.

Responsibility and Authority

The Human Resources Division, County Administrator, and Facilities and Parks Division are responsible for implementing and overseeing this policy.

The Human Resources Division is responsible for issuing ID Cards and Electronic Access Devices with authority granted by the County Administrator. The Facilities and Parks Division, in coordination with the Human Resources Division, will manage access for service contractors in and around the building.

ID Cards

1. Issuing ID Cards

   a. Department Heads shall submit a Request for Access Form for all new Authorized ~~Personnel~~Workforce members as defined above or when any of the above changes in status, departments or positions.

   b. The Facilities and Park Division will manage, authorize and issue ID Cards for all Project and Construction Contractors.

   c. The Human Resources Division shall take photos, or authorize photos to be taken, for ID Cards. The photos shall remain the property of Chippewa County.

   d. Authorized ~~Personnel~~Workforce members shall be issued an ID Card within two (2) business days after new employee orientation and required paperwork has been completed.

   e. Authorized ~~Personnel~~Workforce members shall sign the Identification and Access Policy Acknowledgement form prior to receiving their ID Card.

   f. The Human Resources Division maintains a current list of individuals with ID cards.

g. Because appearances change over time, all Authorized ~~Personnel~~Workforce members may be issued an updated ID Card and new photo as determined periodically by the Human Resources Division.

2. Displaying ID Cards

a. All Authorized ~~Personnel~~Workforce members shall wear their assigned ID Card while in county facilities during their scope of employment/services for Chippewa County. Authorized ~~Personnel~~Workforce members will prominently display the ID Card in a visible location on the front of their person above waist height and to be worn outside clothing.

b. ID Cards shall not be defaced or altered with stickers, decals, etc. Additionally, ID Cards may be worn at seminars and/or conferences or similar County activities when conducting official County business.

c. Failure to wear the ID Card may result in disciplinary action up to and including termination.

d. Exceptions to requirement of wearing County ID Card:

1. Authorized ~~Personnel~~Workforce members in uniform with their name and County identification visible on their uniform are not required to wear a County ID Card. However, they shall carry a County ID Card and display it upon request. Law enforcement officers on covert assignments are exempt from either requirement.

2. Authorized Workforce members who are engaged in construction type work or engaged in an activity where a displayed ID Card could become snagged or cause a safety concern are excluded from the requirement to wear an ID Card while employed in such activity. Such Authorized ~~Personnel~~Workforce members shall however carry the ID Card on their person, and wear it upon ceasing the activity.

3. Forgotten ID Cards

a. If an Authorized ~~Personnel~~Workforce member reports to their assigned County facility without their ID Card, the Department Head/Manager may send the Authorized ~~Personnel~~Workforce member home to retrieve their ID Card, and shall be required to use their available PTO for the absence.

b. The Human Resources Division may issue the Authorized ~~Personnel~~Workforce member a temporary ID Card for that day only upon the request of the Department Head/Manager. Repeated instances may result in disciplinary action up to and including termination.

c. Temporary ID Cards shall be good for one day and shall be returned to the Human Resources Division before leaving the facility at the end of the day.

4. Replacement of County ID Cards/Charges

a. A temporary ID Card may be provided for up to one week prior to issuing a permanent ID Card to allow the Authorized ~~Personnel~~Workforce member time to locate a lost ID Card, if applicable.

b. The Human Resources Division will determine if a replacement ID Card shall be issued at no cost to the Authorized ~~Personnel~~Workforce member or a charge of $15.00.

c. The following are examples where a replacement ID Card may be issued at no cost to the Authorized ~~Personnel~~Workforce member:

1. A replacement ID Card is required for a change in name or employee number at no cost to the Authorized ~~Personnel~~Workforce member.

2. A replacement ID Card may be issued at no cost to the Authorized ~~Personnel~~Workforce member if the ID Card becomes damaged or is otherwise unserviceable due to the scope of employment/services and shall be returned to the Human Resources Division for replacement.

d. The following are examples where an ID Card may be issued at a cost to the Authorized ~~Personnel~~Workforce member at a cost of $15.00 to be paid directly to Chippewa County and submitted to the Human Resources Division upon pick up of the replacement ID Card:

1. Replacement of an ID Card for personal reasons will be issued to the Authorized ~~Personnel~~Workforce member at a cost of $15.00 as determined by the Human Resources Division. The Authorized ~~Personnel~~Workforce member may have a new photo taken for the replacement ID Card.

2. A replacement ID Card may be issued to the Authorized ~~Personnel~~Workforce member at a cost of $15.00 as determined by the Human Resource Division if the ID Card has become lost, damaged or otherwise unserviceable due to prohibited use, defined under section 7 (Prohibitions).

5. Reporting Missing/Stolen/Damaged/Malfunctioning ID Cards

a. For the security and protection of Authorized ~~Personnel~~Workforce members, county facilities, and the data maintained and stored within, all missing, damaged or stolen ID Cards shall be reported immediately to the Department Head/Manager and the Human Resources Division.

6. Project and Construction Contractors

a. When Project or Construction Contractors perform services in County facilities, the department that has retained their services shall coordinate with the Facilities and Parks Division to ensure that the contractor is issued an ID Card identifying them as a Project or Construction Contractor.

b. The Project or Construction Contractor ID Cards shall be a temporary ID card that is generic, with an identification number and does not have a photo. Contractor ID cards

are important for easy identification of who is an approved Project or Construction Contractor vs. an Authorized ~~Personnel~~Workforce member.

c. The department that retained the services of a Project or Construction Contractor is responsible for returning the Contractor ID card as the individual(s) leave the premises.

d. The Facilities and Parks Division shall maintain a list of individuals with Project or Construction Contractor ID cards.

7. Prohibitions

a. Do not give or lend your ID Card to any other individual.

b. Do not leave your ID Card in a location subject to damage, loss or theft.

c. Do not leave ID Cards on the dash of your vehicle or other locations where it may be exposed to extreme temperatures.

d. Do not fold, bend, pry open, alter, mutilate, or fabricate your ID Card.

e. Do not use your ID Card as an ice scraper.

f. Do not wear ID Badges at non-county related events.

Electronic Access

As established in the Chippewa County Code of Ordinances the normal recognized hours of operation for the Chippewa County Courthouse are Monday – Friday, 8:00 a.m. – 4:30 p.m.; closed weekends and holidays. As a result, there is access to the common areas of the Courthouse Monday – Friday, 7:30 a.m. – 5:00 p.m. For those who have business in the courthouse after normal business hours, access is limited to East Entrance #3 and North Entrance #4. Authorized ~~Personnel~~Workforce members may be issued additional specific access to gain entry to the Courthouse and secured area(s).

1. Issuing Electronic Access Devices

a. Access requested and provided is limited so that only the minimum necessary number of individuals are able to access the Courthouse or a Secured or Restricted Area.

b. Authorizing Access – Authorized ~~Personnel~~Workforce members are assigned an Electronic Access Device based on the operational needs to access the Courthouse or a Secured Area. Access is recommended by the Department Head and approved by the Human Resources Director in conjunction with the County Administrator.

c~~b~~. Temporary Access – Department Heads or Managers may request a temporary Electronic Access Device for an employee for short term operational needs, during situations when permanent access to that area is not normally needed or has been denied. Temporary access shall be requested at least three (3) business days in advance to the Human Resources Division. Failure to provide this required notice may result in a delay in receiving the temporary access.

~~c~~d. Emergency Access – Authorized ~~Personnel~~Workforce members that need emergency access shall contact the Sheriff's Department for access. The Sheriff's Department will require a Chippewa County ID Card to confirm the person is an Authorized ~~Personnel~~Workforce member. The Sheriff's Department shall report all requests for emergency access to the Human Resources Division. The Sheriff's Department may contact the Human Resources Division or the Department Head for verification or require a Sheriff's Department escort.

e~~d~~. Authorized ~~Personnel~~Workforce members shall sign the Identification and Access Policy Acknowledgement form prior to receiving their Electronic Access Device.

f. The Human Resources Division shall maintain a current list of individuals with Electronic Access Devices and the access that is activated on them.

g. The Human Resources Division shall:

1. Review physical access logs (e.g. Electronic Access Device audit logs and hard copy / handwritten logs) on a monthly basis to identify any potential unauthorized physical security access.

2. Report and investigate potential and known physical security access.

2. Employee Expectations

a. Authorized ~~Personnel~~Workforce members are responsible for the reasonable care and maintenance of their assigned Electronic Access Device and should safeguard it from damage, loss or theft.

b. Authorized ~~Personnel~~Workforce members who have access to the facility outside of normal business hours shall only access the facility for operational purposes.

c. Notify the Human Resources Division immediately if an Authorized ~~Personnel~~Workforce member's Electronic Access Device is lost or stolen. If the Electronic Access Device needs to be disabled outside of normal business hours, contact the Sheriff's Department immediately.

d. Notify the Human Resources Division immediately if an Authorized ~~Personnel~~Workforce member's Electronic Access Device is broken or is not functioning properly.

3. Prohibitions

a. Do not give or lend your Electronic Access Device to any other individual.

b. Do not leave your Electronic Access Device in a location subject to damage, loss or theft.

c. Do not leave your Electronic Access Devices on the dash of your vehicle or other locations where it may be exposed to extreme temperatures.

d. Do not pry open, alter, mutilate, or fabricate your Electronic Access Device.

e. Do not allow any non-Authorized ~~Personnel~~Workforce member access to the facility outside of normal business hours when you enter or leave the facility. If you observe any unauthorized or unknown person entering or attempting to gain entry, report immediately to a manager or the Sheriff's Department.

f. Do not hold or prop the facility doors open.

g. Do not store your Electronic Access Device directly with your ID Card.

4. Role Changes

a. When an individual's role changes, the Department Head or Manager shall immediately complete a Request for Access Form and forward it to the Human Resources Division to ensure that the ID and access continues to be appropriate for his/her role.

b. When an individual terminates, the Department Head or Manager shall immediately notify the Human Resources Division to ensure that ID and access is terminated.

c. ID and Access are changed or terminated immediately after receiving the request, but no later than 24 business hours after notification, whether received verbally, via email or in writing.

5. Replacement of County Electronic Access Device

a. If an employee loses or damages their Electronic Access Device, the Human Resources Division will determine if a replacement Electronic Access Device shall be issued at no cost to the Authorized Workforce member or a charge of $15.00.

c. The following are examples where a replacement Electronic Access Device may be issued at no cost to the Authorized Workforce member:

1. A replacement device is required for normal wear and tear by the Authorized Workforce member and is returned to the Human Resources Division.

2. A replacement device is required because the device becomes damaged or is otherwise unserviceable due to the scope of employment/services and is returned to the Human Resources Division.

d. The following are examples where an Electronic Access Device may be issued at a cost to the Authorized Workforce member at a cost of $15.00 to be paid directly to Chippewa County and submitted to the Human Resources Division upon pick up of the replacement Electronic Access Device:

1. A replacement Electronic Access Device may be issued to the Authorized Workforce member at a cost of $15.00 as determined by the Human Resource Division if the Electronic Access Device has become lost, damaged or otherwise unserviceable due to prohibited use, defined under section 3 (Prohibitions).

6. Separation

a. The Electronic Access Device shall be returned to the Human Resources Division by the last day of:

1) Separation of employment
2) Contract service
3) Volunteer service

b. Failure to return your Electronic Access Device shall result in a $15.00 charge.

Reporting and Compliance

Refer to the Information Privacy and Security policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Applicable Standards/Regulations

1. HIPAA Final Omnibus Rule, January 25, 2013
2. 45 CFR §164.310(a) HIPAA Security Rule Facility Access Controls
3. 45 CFR §164.310(a)(2)(ii) HIPAA Security Rule Facility Security Plan
4. 45 CFR §164. 310(a)(2)(iii) HIPAA Security Rule Access Control & Validation Procedures

Chippewa County
Department of Administration
Information Technology Division

Information Technology Policy Manual

County Board History/Action
Adopted by the County Board December 10, 2019

PROPOSED REVISIONS

2. Technology and Information Privacy and Security Policy

2. Technology and Information Privacy and Security Policy

Purpose

The purpose of this policy is to establish a standard for acceptable and authorized use of County-owned and/or County-provided technology. As Chippewa County becomes increasingly dependent on electronic information processing in the course of day-to-day operations, maintaining the Confidentiality, Integrity, and Availability of County information assets, including Confidential Information, is critical to insure sound investment in Information Technology (IT) resources. The scope of this policy includes all authorized users who use and/or access County-owned IT hardware, software, and / or network resources. Authorized users as referred to in this policy shall include Workforce, elected officials and all users of County hardware and/or software.

Definitions

The HIPAA Privacy and Security terms utilized in this policy are capitalized throughout the document. The definitions of those terms are located in a document titled HIPAA Privacy and Security Definitions found on the Employee Portal and maintained by the Privacy and Security Officers.

Responsible for Implementation

The Security Officer and Information Technology Director are responsible for implementing and overseeing this policy and procedure

Policy

1. User Accounts and Passwords

   The assignment of unique user accounts and passwords to authorized users, including administrator accounts, will be made by the IT Division for the appropriate information system(s) and Workstations being accessed.

   County user accounts and/or passwords shall be safeguarded from unauthorized use and may not, under any circumstance, be written down in a public and/or conspicuous location. Passwords shall only be known by the individual user. Passwords may not be shared with anyone, including friends, family, co-workers, etc. Users may not:

   a. Reveal a password over the phone or in an e-mail to anyone.

      1. A user may share a user ID and password with the IT Division when they have a legitimate need to fix a system issue.

      2. When this is done the IT Division will require the password be changed immediately after this issue has been resolved.

b. Leave user names (UNs) and passwords (PWs) so someone else may see or find them.

c. Use their UNs & PWs to log other individuals into the system.

d. Use the UNs & PWs of others or any Information System logged in under another user's UN & PW.

e. Store passwords electronically unless they are encrypted and password protected, nor written down unless they are locked and accessible only to the owner.

Users are responsible for all inquiries, entries, and changes made to any of the organization's Information Systems using their UNs & PWs.

Users that do not recall their UN & PW contact the IT Division or IT Help Desk. The IT Division or IT Help Desk shall:

a. Validate the user's identity

b. Verbally provide the user with a temporary, one-time use UN & PW

Additional Password Requirements:

a. At a minimum, smart phones require a six character unique pass code.

b. Servers store private encryption keys and are protected by a VPN with a password.

c. Refer to the Unique User IDs, Passwords, and Configurations Policies and Procedures for requirements for Workstations integrated with Active Directory settings.

d. For Information Systems, refer to the Unique User IDs, Passwords, and Configurations policy for password configuration settings and requirements.

2. Log-off

Users are required to lock or logoff Workstations, portable devices, and/or Information Systems when left unattended (whether on or off the premises) for any amount of time, so that Confidential Information is inaccessible by any other individual. Personal computers and laptops may be locked by simultaneously pressing the Windows and L keys on a keyboard.

If a device is used only by a single individual with a unique log in, it may be locked and information systems on that device may remain logged in.

Users are required to log off systems and shut down workstations at the end of the work day, unless running a job on it.

Workstations automatically lock after a minimum of 15 minutes of inactivity (smart phones after two (2) minutes of inactivity; squad car MDCs after eight (8) hours).

a. This feature is set by the IT Division or System Administrators and may not be changed by users.

b. The user's password must be used to re-establish the session.

c. Exceptions are authorized and documented by the IT Division.

Information Systems that create, receive, maintain or transmit, or otherwise provide access to Confidential Information, whenever possible:

d. Automatically log users off the applications after a minimum of up to 180 minutes of inactivity.

e. Invalid attempt automated account locks

1. Automatically lock accounts after three invalid login attempts within five (5) minutes.

2. The user account locks for a period of thirty (30) minutes (or locks until a System Administrator unlocks it). After this period, the bad password count is reset to zero (0) and the user can attempt to log on.

3. System Administrators have the ability to unlock accounts at any time.

VPN, Citrix, and other software application sessions automatically terminate after thirty (30) minutes of inactivity.

3. Software

The Chippewa County IT Division is responsible for the purchase and installation of all software. Users may not download any software to a County Workstation. Illegal copying of software is not permitted. Personally-owned and/or unlicensed software may not under any circumstance be loaded or installed onto County-owned systems. Unapproved software may be removed without advance notice to the user.

Software programs and applications must be licensed by the County. The IT Division maintains the licensing information.

4. Hardware

The Chippewa County IT Division is responsible for purchasing all hardware. Personal Workstations and Electronic Media may not be connected to County owned Workstations, devices, Electronic Media or the network, unless authorized in writing by a Department Head or member of the Management Team and IT Division.

5. Requests to Access Confidential Information

Members of the management team are the only individuals authorized to request access for users to Confidential Information. Role based access requests are submitted to the Human Resources Division. The IT Division sets up, changes, and terminates user accounts based on these requests.

6. Internet and Online Services

Electronic transmissions or communication via the Internet shall not be considered either private or completely secure.

The Internet offers numerous discussion groups or forums and exchange ideas for the purpose of research and information sharing. As with any form of communication, the County shall not be intentionally misrepresented in any material posted to the Internet.

Authorized users are responsible to ensure the content of material they transmit or publish in electronic communications or messages via County-provided Internet access, email, information systems, and Workstations is appropriate. Hate mail, harassment, discriminatory remarks, profanity, antisocial, disrespectful or unprofessional behavior such as targeting another person or organization to cause distress, embarrassment, injury, unwanted attention or other substantial discomfort is prohibited. Personal attacks or other action to threaten or intimidate or embarrass an individual, group or organization or attacks based on a protected class or any other such characteristic or affiliation are prohibited. Illegal communications are also prohibited.

County Internet usage is logged and accessible by designated staff, as appropriate. Internet usage and history may be subject to public inspection.

7. Electronic Mail Communications (Email)

Business communication via email allows the sender and receiver to be flexible, decide on an appropriate time to address something, not disrupt operational work flows, and in some cases multi-task. Senders should consider the audience, the tone, grammar, and punctuation within the message, and must also consider that any email has limitations as a communication tool. For that reason, senders should use sound professional judgment when determining if email is the most appropriate form of communication for the message they are sending.

Standard emails are inherently not a secure method of communication and can, therefore, be intercepted by unauthorized individuals.

Email is subject to applicable privacy, security, open records and records retention laws and guidelines, as are appropriate, for the information that a particular message contains. It is important to remember that you are creating a government document simply by creating and sending an email.

Chippewa County will archive all email and employ the use of an email archival method to retain all messages sent and received to and from the County email system as identified in the record retention ordinance.

Authorized users are not permitted to print, display, download or send sexually explicit images, messages, or any other material disparaging or harassing to anyone. If such material is received, and if feasible, recipient shall immediately advise sender that receipt of such transmission is not permitted and must stop. If assistance is needed in responding to the receipt of inappropriate material, the matter is to be referred to the Human Resources Division.

Users are responsible to ensure the content of material they transmit or publish in messages via County-provided email access is appropriate. Users may not send, request, reply to, or forward chain letters/emails. Refer to the Internet and Online Services and Prohibited Use of Technologies sections of this policy for prohibited electronic communications / messages and additional protection requirements.

Clients and consumers whom request a copy of their Designated Record Set (as defined in 45 CFR 164.501) be emailed are referred to the appropriate Records Department. The Records Department processes the request as described in Release of Information policies.

Users authorized to email Confidential Information to individuals whom are authorized to receive the Confidential Information:

a. Are required to use the email encryption program provided by the County. When emailing the Confidential Information type "secure" in the subject line for external emails; this encrypts the email

b. Do not include any PHI, such as client, consumer or subscriber identifiers, in the subject line. These include, but are not limited to the following:

    1. Full Name
    2. Date of Birth
    3. Social Security Number
    4. MCI Number
    5. Address
    6. Telephone Number

c. Before sending the email, verify that you are sending it to the correct individual(s) and that the email is/will be encrypted.

Users may not open any suspicious emails or suspicious website links in emails. If uncertain an email and/or email attachment is suspicious, delete the email or personally call the sender at a known telephone number. If uncertain a website link is suspicious, do not click on it. Instead, open the website from a saved favorite list or do a website search.

8. Remote Email Access

Chippewa County permits the use of secure, remote email access via external Internet connection to the County email system. Example: Microsoft Outlook Web Access (OWA).

Remote email access and use is provided to conduct County-related business. Authorized users are permitted, however, to use Chippewa County's technical resources, including remote Email Access, for occasional, appropriate and minimal non-work is subject to department approval.

All remote email access users are required to honor and observe the rules of confidentiality and protection of privacy when accessing and using any information that resides on the Chippewa County email system. Remote email access may be used only while an authorized user retains authority from the department head or elected official. It is the responsibility of the Department Head/Elected Official to notify the Human Resources Division of any Workforce member changes that require disabling access to IT services. Service may be limited, suspended or terminated in cases of suspected or known wrongdoing, with or without notice to a user.

All remote email access use by non-management Workforce member is required to have prior approval from the Department Head or Elected Official for remote email access outside of the Workforce member's approved scheduled work time. Use of remote email access without prior approval that results in additional hours worked by non-management Workforce is prohibited.

9. Remote Virtual Private Network (VPN) Access

Chippewa County allows remote VPN access on county issued hardware for management Workforce member only. No personal home computers or other devices are allowed to be used to VPN into the county systems (some exceptions may be approved by the HR Director or IT Director). Requests for a VPN connection must be initially approved by the Department Head/Elected Official. All initially approved requests for employee VPN access shall be submitted to the Human Resources Director for final approval. All other initially approved VPN access requests shall be submitted to the IT Director for final approval.

Remote access service is provided to conduct County-related business. Authorized Workforce members are permitted, however, to use Chippewa County's technical resources, including remote access service, for occasional, appropriate and minimal non-work purposes.

All authorized Workforce members of County-provided remote access services are required to honor and observe the rules of confidentiality and protection of privacy when accessing and using any information that resides on Chippewa County systems. Workforce members agree to apply safeguards to protect County information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remote access service, prevention of inadvertent or intentional viewing of displayed or printed information by unauthorized individuals. Service may be limited, suspended or terminated in cases of suspected or known wrongdoing, with or without notice to a user.

10. Offsite (Remote) Security Safeguards

a. Remote access is a privilege, and is granted only to remote users who have a defined need for such access and who demonstrate compliance with the County's

established safeguards which protect the Confidentiality, Integrity, and Availability of Confidential Information.

b. Individuals may not take electronic Confidential Information off of the County's premises, unless allowed by the County's policies. When electronic Confidential Information is authorized to be taken offsite, individuals are required to secure the information as stated in the County's policies to prevent unauthorized access, use, and disclosure of it.

c. Authorized users may access ePHI remotely to perform assigned job responsibilities

d. Individuals may not take hard copy (paper) PHI or other Restricted Information offsite, unless specified below:

1. CCDHS and CCDPH client and consumer files shall be allowed at court proceedings, as appropriate for the court proceedings.

2. CCDHS and CCDPH client files (e.g. aide sheets, assessment forms, etc.) may be taken offsite as needed to provide services in the community.

3. Other Exceptions are approved and documented by the Privacy Officer.
4. When hard copy (e.g. paper) PHI other Restricted Information is authorized to be taken offsite, it shall be secured at all times by being in the possession of and/or in a locked container at all times so that only authorized individuals have access to the information. If must be left in a vehicle, lock it and place them in the trunk (or if there is not a trunk in an area that is out of plain sight).

e. Treatment Records may not be taken offsite, except by Workforce members directly involved in the patient's treatment, or as required by law. Note: this is from WI DHS 92.04(6)(c) and applies to Treatment Facilities (treatment of Alcoholic, Drug Dependent, Mentally Ill or Developmentally Disabled persons).

f. Remote users are responsible for:

1. Adhering to all of the County's privacy and security policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for the County's 's approved business purposes.

2. Troubleshooting of telephone or broadband circuits installed. It is not the responsibility of the County to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by the County.

3. Ensuring that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

4. Using the County's VPN, or other approved transmission method, to transfer Confidential Information.

g. Remote users must:

1. Manage documents and equipment that contains and/or transmits Confidential Information as described in the County's privacy and security policies.

2. Have and use a paper shredder and follow the Disposal of Confidential Information policy, or bring the Confidential Information in to the office to dispose of appropriately.

3. Secure office environments and prevent visitors and family from viewing, accessing, and hearing Confidential Information.

4. Secure Confidential Information in a locked file cabinet when unattended and not in use.

5. Log-off and disconnect from the County's network when access is no longer needed to perform job responsibilities.

6. Lock the workstation and/or system(s) when unattended so that no other individual is able to access the County's network or Confidential Information.

7. Not copy Confidential Information, including ePHI, to personal media (hard drive, USB, cd, smart phone, tablet, laptop, personal computer, etc.), unless the County granted prior written approval.

11. Texting, ~~and~~ Instant Messaging, Paging Via a Pager, and Overhead Paging

Texting, ~~and~~ Instant messaging, paging via a pager, and overhead paging are unsecured methods of communication and can, therefore, be intercepted by unauthorized individuals.

As the County does not have a means to encrypt texts, Confidential Information may not be texted at any time from any device, whether or not the texting device is owned by the organization.

As the County does not have a means to encrypt instant messages, Confidential Information may not be sent through an instant message at any time from any device, whether or not the instant messaging software and/or device is owned by the organization.

As the County does not have a means to encrypt pages via a pager, Confidential Information may not be sent through a pager at any time from any device, whether or not the paging device is owned by the organization.

As the County does not have a means to encrypt overhead paging, Confidential Information may not be stated through an overhead paging system at any time from any device, whether or not the paging device is owned by the organization.

12. Virtual Meeting Platforms

Only virtual meeting platforms managed by the IT Division may be utilized. Webex, Zoom, and Microsoft Teams, managed by the IT Division, may be used for internal workforce meetings, general internal communications, and scheduling meetings with vendors. Native smartphone video platforms may be utilized on County provided devices (i.e. FaceTime, Duo, etc.). Note: vendors and other organizations may send invitations to Chippewa County workforce utilizing their own platforms which may be utilized to attend virtual meetings.

No virtual meeting platform may be used to transmit Confidential Information at any time via a chat / message, with the exception of telehealth services provided consistent with any County policy.

~~12~~13. Prohibited Use of Technologies

The following items and activities concerning County-owned and/or County-provided technology are expressly prohibited:

a. Engaging in any activity which violates state law, federal law, County Policy, County Administrative Code, the Civil Service Rules or departmental work rules, as applicable.

b. Engaging in activities during working hours for personal gain, solicitation or commercial purposes, including commercial advertising, unless specific to the mission or duties of the applicable Department or County.

c. Accessing or distributing indecent material, obscene material, child pornography or any material that violates County's affirmative action principles or the civil rights (of protected class) of an individual.

d. Harassing other individuals, including sending chain letters or inflammatory material.

e. Loading personally-owned or improperly licensed software on County-owned equipment.

f. Loading software of any kind is not allowed. All installs are to be completed by the IT Division.

g. Moving equipment from one location to another. While laptops are meant to be mobile and used in various locations, they may not be permanently moved to different offices / locations.

h. Obligating the County for user fees, usage charges or membership fees without prior authorization.

i. Deliberately damaging computing systems or altering the software components of County-owned systems.

j. Engaging in any activity which adversely affects the Availability, Confidentiality or Integrity of any County-provided technology and data.

k. Disseminating or printing copyrighted materials (including articles and software) in violation of copyright laws.

l. Disseminating information that is known to misrepresent the County or be false, inaccurate or misleading.

m. Using another's network, Internet, electronic mail or online service account or password without authorization.

n. Sending of Confidential Information through an external network transmission (e.g. email system, instant messaging application, VPN, etc.) that was not set up and monitored by the IT Division or designee.

o. Deliberately compromising computer and/or network security.

p. Sending disrespectful or unprofessional business communication that causes distress, disruption, embarrassment, injury, or unwanted attention or other substantial discomfort to the recipient.

q. Allowing any other individual to use any of the organization's Workstation's or Information Systems that is not authorized by the organization to utilize them

r. Downloading any Confidential Information off the County's Information Systems, Workstations, servers, etc. to store or use it on any Information System, file sharing site, Workstation, compact disc, digital video disc, zip disc, or other portable devices or removable storage devices such as removable USB or flash drives that is not authorized by the IT Division. Users that receive approval to download data onto approved equipment or Information System are responsible for managing and protecting it from unauthorized access, disclosure, and theft.

s. Activating a white board, camera, microphone, or any other type of collaborative computing device unless it was authorized and/or set up by the IT Division. These must show an indication to users that they are turned on, being used, and/or are activated, such as with a light or pop-up alert.

t. Using or making available file sharing or peer to peer networks (Windows file shares, torrent, kazaa, limewire, etc.) or extending the County's network (example: wireless access points).

u. Using tools or techniques to break/exploit or disable security measures.

v. Change operating system configurations, upgrade existing operating systems, or install new operating systems.

w. Connect to unauthorized networks through the organization's systems or devices.

x. Connecting a Workstations (including portable devices) to the organization's network and wireless network that was not authorized by the IT Division

y. Overload any computer system or network.

~~13~~14. Ownership of Resources

Email, Internet, information system, Workstations, and telecommunication access are resources made available to County authorized users to communicate with each other, other governmental entities, companies and individuals for the benefit of the County.

All Workstations purchased by the organization are the property of the County. Users do not own any information accessed or created during their relationship with the County on these Workstations or information systems provided by the County. The County owns it. Designated staff from the County reserve the right to examine all email, directories, files and other information stored on all County-owned data disks, computers, tape or other media and to monitor all email, Internet, computer system and telecommunication access and activity as deemed necessary.

Authorized users have no right of privacy in anything they create, store, send or receive using the County's technologies. Anything created using county technologies may be reviewed by others.

~~14~~15. Rights of Chippewa County

a. The County owns all technologies provided at its own expense or under its authority or jurisdiction, including transmissions initiated, received or stored using its technologies.

b. The County reserves the right to determine who is provided access to its Workstations, servers, systems, network and technologies.

c. At any time and without prior notice, the County may remove any user account.

d. The County may monitor and/or log network use, capacity and space utilization.

e. At any time, the County may access or examine electronic mail and/or monitor messages on its equipment, Information Systems, or networks.

f. At any time, the County may access or examine files or any other materials stored on its equipment or networks.

g. At any time, the County may monitor and audit any user's access to all of the organization's Workstations, portable devices, servers, Information Systems, Internet activities, and applications.

h. The County may archive or delete files or any other materials on its equipment or networks, as deemed necessary.

~~15~~16. Confidentiality

The County uses and stores Confidential Information in various forms throughout the facilities that is used to provide services to the community. All Confidential Information is the property of the County. Certain Workforce members and/or contract workers may be required to sign a confidentiality agreement form for the department they work in. Unauthorized release, distribution or copying of confidential information is prohibited.

Protecting information assets and systems rests on all users and, therefore, all users are accountable for their actions. All users of information assets or systems must take appropriate care to ensure that the information assets/systems they use in the course of their work are protected from unauthorized access, use, disclosure, modification, and destruction.

When approached by an individual that may be able to view Confidential Information to which they are not authorized, users minimize the Information System or otherwise secure it so that the individual is not able to view the Confidential Information.

Workstations are placed in secure areas away from regular client, consumer or subscriber traffic and display screens are positioned to minimize unauthorized viewing and/or access, whenever feasible.

County issued mobile devices may be taken offsite. Other types of Workstations (e.g. desktop computer) may be taken off the premises when approved by a Department Head and IT Director. When Confidential Information is stored on them, all Workstations must be encrypted. The IT Division maintains a list of each Workstation issued to individuals.

When authorized to remove Workstations (including mobile devices and desktop computers) from the premises:

a. Protect them with security controls equivalent to those for on-site Workstations/mobile devices.

b. When transporting these Workstations /mobile devices as applicable:

1. Place them in closed bags.

2. Place them in the trunk of vehicles (if there isn't a trunk, in an area that is out of plain sight) when unattended for short periods of time; do not leave them in a vehicle overnight

3. Do not leave them in a vehicle during extreme hot or cold temperatures.

4. Take them as carryon luggage when traveling.

Save / store all information on the County's network drives, not on Workstations or flash / USB drives. This ensures information is sufficiently backed up and secured. PHI may not be stored on flash / USB drives except for when the Privacy Officer agrees to a client, consumer, or subscriber access to records request. Note that data stored locally on desktop computers, laptops, other personal Workstations, and flash / USB drives are not backed up. If it is necessary to store information on a Workstation, such as when traveling or a network drive is not currently available, obtain approval from and coordinate with a Department Head and IT Division to ensure the information is sufficiently backed up and encrypted.

All users are responsible for practicing precautions to protect the Confidentiality, Integrity, and Availability of Confidential Information at all times. Users are required to monitor Workstations and take measures to prevent unauthorized access and theft.

Users may only access, use, and disclose the Minimum Necessary Confidential Information:

c. When needed to perform assigned job responsibilities

d. As allowed by County policies and procedures

e. As allowed by law

Users are required to comply with all applicable information security policies, standards and procedures to ensure that the County's Information Systems and assets areas are protected.

Users may not access their own, a family member's, friend's, or relative's PHI on paper or in any Information System without prior authorization from their Department Head and as allowed by the organization's policies.

~~16~~17. Dual Relationships

a. When users have a personal relationship with a client, consumer, subscriber (past or present), efforts shall be made to avoid a dual relationship including eliminating records accessed by that users as well as limiting case assignment (as software capabilities allow) by a user member to that person.

b. Record access and case assignment shall be determined on a case by case basis subject to approval of the program manager.

c. When a client, consumer, subscriber expresses that they view it as a dual relationship or conflict of interest and evidence supports a past or present relationship – it is viewed as such.

d. If one of these individuals needs care, request a co-worker to take care of the client, consumer, subscriber.

e. If it is an urgent care situation and nobody else is available to help, provide care and inform their Department Head in the organization of the situation.

f. Any users who becomes aware of a potential dual relationship or conflict of interest shall immediately divulge this information to their Department Head.

~~17~~18. Data Backups

a. Data that is stored locally on desktop computers, laptops, and other personal Workstations are not backed up.

b. Data that is stored on systems that are not managed by the Information Technology department are not backed up.

c. Only Workforce and vendors / Business Associates authorized by the Information Technology Director are allowed to perform backups.

~~18~~19. Contingency Plan

a. Workforce members are required to report when systems and networks are down, or suspect a potential business continuity threat.

b. Workforce members are also expected to cooperate with Contingency Plan / Disaster Recovery efforts.

~~19~~20. Integrity

a. The County utilizes various methods to protect Confidential Information from improper and/or unauthorized alteration or destruction and validate that this hasn't happened until properly disposed.

b. To assist with Integrity related controls, users:

1. May only change/amend Confidential Information in Information Systems and on their Workstations as described in amendment of PHI policies and procedures.

2. During the regular course of their job responsibilities, are required to check for and report any errors or potential errors of Confidential Information identified in Information Systems to a member of the management team.

~~20~~21. System Build / Change Control

a. Changes to the information technology infrastructure (e.g. changing, purchasing, or otherwise introducing new applications or technologies into the information technology production environment) may only be done by Workforce and vendors / contractors authorized by the IT Division.

b. System builds, changes, and work necessary to follow and implement security baseline standards are completed, or at a minimum supervised, by individuals with minimum skill sets needed to complete the work.

c. Refer to the System Build / Change Control policy for additional system build / change management requirements.

Applicable Standards/Regulations

- 45 CFR § 164.308(a)(1)(ii)(D) HIPAA Security Rule Information System Activity Review
- 45 CFR §164.308(a)(3)(i) HIPAA Security Rule Workforce Security
- 45 CFR §164.308(a)(4)(i) HIPAA Security Rule Information Access Management
- 45 CFR §164.308(a)(4)(ii)(B) HIPAA Security Rule Access Authorization
- 45 CFR §164.308(a)(4)(ii)(C) HIPAA Security Rule Access Establishment and Modification
- 45 CFR § 164.308(a)(5)(ii)(C) HIPAA Security Rule Log-in Monitoring
- 45 CFR §164.308(a)(5)(ii)(D) HIPAA Security Rule Password Management
- 45 CFR § 164.308(a)(7)(ii)(A) HIPAA Security Rule Data Backup Plan
- 45 CFR § 164.308(a)(7)(ii)(B) HIPAA Security Rule Disaster Recovery Plan
- 45 CFR §164.310(b) HIPAA Security Rule Workstation Use
- 45 CFR §164.310(c) HIPAA Security Rule Workstation Security
- 45 CFR §164.312(a)(2)(i) HIPAA Security Rule Unique User Identification
- 45 CFR §164.312(a)(2)(iii) HIPAA Security Rule Automatic Logoff
- 45 CFR §164.312(a)(2)(iv) HIPAA Security Rule Encryption and Decryption
- 45 CFR § 164.312(b) HIPAA Security Rule Audit Controls
- 45 CFR. §164.312(c)(1) HIPAA Security Rule Integrity
- 45 CFR §164.312(c)(2) HIPAA Security Rule Mechanism to Authenticate Electronic PHI
- 45 CFR §164.312(d) HIPAA Security Rule Person or Entity Authentication
- 45 CFR §164.312(e)(1) HIPAA Security Rule Transmission Security
- 45 CFR §164.312(e)(2)(ii) HIPAA Security Rule Encryption
- 45 CFR §164.312(e)(2)(i) HIPAA Security Rule Integrity Controls

** NEW POLICY **

DATA BACKUP AND MEDIA MANAGEMENT POLICY AND PROCEDURES

Purpose

Backing up Electronic Protected Health Information (ePHI) and other Restricted Information, as well as Sensitive Information, collectively "Confidential Information", and the correct storage of it are an important part of the day-to-day operations of the organization's information security program.

The primary purpose for system backups is to avoid any data loss due to hardware failure, computer virus attack, or any disaster situation that could cause data loss on the network servers, and services provided by network servers (e-mail, databases, etc.). In addition, the backup system allows the ability to provide file restoration for user files that are stored on networked servers. Backups are done so that information is available as needed, even during system failures and emergencies (as feasible). Guidelines are established to track the movement of Hardware and Electronic Media containing Confidential Information to help maintain the confidentiality, integrity and availability of it.

Responsible for Implementation

It is the responsibility of the IT Director for implementing and overseeing this policy and procedures.

The IT Division is responsible for overseeing and delegating Confidential Information data Backups and logging and monitoring of movements of Hardware and Electronic Media containing Confidential Information.

Policy

1. It is the policy of Chippewa County (herein County) to establish and implement procedures to create and maintain retrievable exact copies of Confidential Information.

2. To assure that complete, accurate, retrievable, and tested back-ups of Confidential Information are available for all information systems used by the organization, as needed.

3. To create a retrievable exact copy of Confidential Information before movement of equipment.

4. To maintain a record/log of movements of Hardware and Electronic Media containing Confidential Information.

Procedures

1. <u>Data Backups – General Requirements</u>

   a. Refer to the Technology and Information Privacy and Security policy in the IT Policy Manual – Data Backups section for general Backup requirements.

2. <u>Confidential Information Data Backup</u>

   a. Performing Backups:

1. Individuals responsible for data Backups are trained by individuals experienced on the procedures to complete these Backups, before being allowed to complete a Backup.

2. When Confidential Information Backups are completed and/or stored by a vendor:

   a). The vendors are required to have the below stated controls in place, at a minimum.

   b). A Business Associate Agreement is in place, as required by the Business Associate Policy.

   c). Also refer to the Service Providers policy for additional requirements.

b. Detailed procedures describing how to Backup systems are documented and maintained by the IT Division and include:

1. System name
2. Type of information backed up
3. Live data storage location
4. Backup storage location
5. Backup frequency
6. Class of information backed up
7. Backup retention period, including daily, weekly, monthly, quarterly, and annual backups
8. Type of encryption used for the transmission and storage media
9. Documentation confirming when backups were completed
10. Process to validate proper execution and success of each backup
11. Process to respond to and track each issue found or reported via alerts for all backups and insure prompt response and remediation and successful re-execution of failing backup
12. How to recover data from backups
13. Required backup restoral tests process, intervals and tracking to confirm complete backup and restoral integrity

c. Reasonable efforts are made to utilize the following backup controls, at a minimum:

1. Backup types and frequency.

   a). Virtual servers:

      1). Perform Backups in in a manner that the information system or asset can be fully restored on or offsite to ensure availability

      2). Perform hourly asynchronous replication to the backup data center

      3). Daily backups are retained six (6) months

      4). Quarterly full tape backups are retained for two (2) years

      5). Yearly tape backups are retained for two years

6). Domain controllers are backed up nightly

b). Video surveillance servers are not currently backed up.

d. Backup storage:

1. Virtual Backups are performed offsite.

2. Tape backups are stored in a separate building than the servers.

3. To protect them from loss or environmental damage Backups are stored:

a). In an environmentally protected (from fires, water damage, wind damage, etc.) location such as a fireproof, locked safe that is not located next to a water source.

b). In a physically secured location that has a very low probability of being affected by the same disaster as where the live data is stored.

c). So that access is limited to only those key individuals responsible for the Backups and/or recovery of data off the Backups.

e. Transporting of Backups:

1. Confidential Information stored on portable backup storage media is encrypted (refer to the Technical Access Control policy).

2. Backup drives, disks, or tapes and other portable media containing Confidential Information must be protected from unauthorized access and may only be handled by authorized individuals.

3. Backups are transported directly to the backup storage facility.

4. Backups may not be left in an unattended vehicle.

f. Backup software automatically sends email alerts to the IT Division on success, warning, and error backup jobs.

g. Test Backups on a quarterly basis. Document when files have been completely and accurately restored from the back up media.

3. <u>Moving Confidential Information – Electronic Media</u>

It is not possible or economically practical to control all Electronic Media that enter, leave, and are moved throughout the organization and remotely. The organization makes all reasonable and prudent efforts to control Electronic Media entering and leaving the organization. All users are responsible for securing devices when on and off the premises, according to the organization's information security policies. Electronic Media is encrypted as stated in the Technical Access Control Policy.

a. Refer to the Technology and Information Privacy and Security policy in the IT Policy Manual – Confidentiality section for requirements related to removing Workstations from the premises.

b. Prior to moving Hardware or Electronic Media that stores (e.g. such as servers, hard drives, backups, etc.) or transmits Confidential Information, excluding previously approved Workstations, to a new location:

1. Backup a retrievable copy of the Confidential Information, on a separate device when possible. The individual(s) that creates the Backup also manages the Backup Electronic Media as described in the above Confidential Information Data Backup procedures.

2. Record it on a Data Management: Moving Media Log.

3. The IT Division maintains copies of the Moving Media Log.

c. Before disposing of Electronic Media at an offsite location, refer to the Disposal Policy.

4. Documentation

All documentation required by this policy is maintained for six (6) years from the date of creation or the date when it was last in effect, whichever is later.

Reporting and Compliance

Refer to the Information Privacy and Security policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Resources

1. NIST Contingency Planning Guide for Federal Information Systems, SP 800-34 Rev 1, November 2010
2. HIPAA COW Data Management and Backup Policy, version #8, 4/19/05

Applicable Standards/Regulations:

1. 45 CFR § 160.103(a) HIPAA definition of Electronic Media (1/25/13)
2. 45 CFR § 164.308(a)(7)(ii)(A) HIPAA Security Rule Data Backup Plan
3. 45 CFR § 164.310(d)(1) HIPAA Security Rule Device and Media Controls
4. 45 CFR § 164.310(d)(2)(iii) HIPAA Security Rule Accountability
5. 45 CFR § 164.310(d)(2)(iv) HIPAA Security Rule Data Backup and Storage

** NEW POLICY **

MALICIOUS SOFTWARE PROTECTIONS POLICY

Purpose

Malicious software (e.g. viruses, malware, Trojan horses, worms, and ransomware) is hostile and intrusive software that has the ability to breach, alter, delete, destroy, and otherwise make data not available. The purpose of this policy is to put in place general safeguards, technologies, monitoring, procedures and a timely patch management program to effectively prevent vulnerabilities from being exploited as well as reduce risks associated with the introduction of malicious software.

Responsible for Implementation

The Information Technology Director is responsible for developing, approving, and overseeing this policy and procedures. The Information Technology Division responsible for implementing this policy and procedures.

Policy

It is the policy of the County to make reasonable efforts to guard against, detect, report, and remove malicious software through the use of anti-malware software, a timely patch management program, properly configured firewalls, and monitoring.

Procedures

1. General Protections from Malicious Software / Malware

    a. If a virus or other malicious software is detected or suspected, users shall immediately contact the Information Technology Division and cease to use the device and/or system. The Information Technology Division shall research and mitigate it, as well as report it as a Security Incident per the Privacy and Security Incident Response policy (refer to the 416 Information Privacy and Security Policy).

    b. Components and information systems for which anti-malware software and/or patches that are outdated and/or cannot be managed, maintained or updated are on a separate network segment or VLAN.

2. General Technology / Controls

    a. The County utilizes current anti-malware software, a patch management process, and secure firewalls to guard against, detect, report, and remove malicious software.

        1. The Information Technology Division is responsible for maintaining current, effective, and documented anti-malware, patches, and firewalls.

2. The County scans all software and files accessed or downloaded from external sources including, but not limited to the internet, USB drives, floppy diskettes, other portable devices, and network drives before installing or using it (this may be automated or manually done, depending upon the media).

b. The Information Technology Division is authorized to select and use tools that are designed to detect network vulnerabilities and intrusions. Use of such tools by others are explicitly prohibited without the explicit authorization of the Information Technology Director. These tools may include, but are not limited to:

1. Vulnerability testing software to probe the network to identify what is running (e.g., operating system or product versions in place), assess whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls. Refer to the System Build / Change Control policy.

2. Scanning tools and devices.

3. War dialing software.

4. Password cracking utilities (only utilized in extreme / critical cases).

5. Network “sniffers”.

6. Passive and active intrusion detection systems. Refer to the Intrusion Detection standard.

7. External auditors hired are independent of other organizational operations, have technical expertise in the type of audit conducted, and sign a Business Associate Agreement.

3. Anti-malware software

a. Anti-malware software is on all servers, Workstations, portable devices, and email applications.

b. Users may not turn off or disable anti-malware systems.

c. Refer to the Malware Standard for baseline implementations and scanning requirements.

d. To verify anti-malware software is installed and current, auditing is completed for each type of device/electronic media, automated mechanisms and reporting are in place and a status review shall be completed on a weekly basis.

4. Patch management

a. A patch management process is in place to promptly identify risks posed by software security vulnerabilities and take appropriate actions to mitigate them.

b. Patching procedures adhere to the System Build / Change Control policy and procedures.

c. For systems and components managed by the County, the Information Technology Division and/or System Administrators shall:

1. Subscribe to and monitor industry-accepted third-party vulnerability notifications (e.g. vendor websites, industry news groups, mailing lists, or RSS feeds).

2. Monitor for Information System, Workstation, Electronic Media, hardware device, firmware, and other system component security patches, hot-fixes, service packs, and/or zero-day vulnerabilities on a weekly basis at a minimum.

3. Determine and document when it is acceptable to automate patches (e.g. for non-mission critical applications and operating systems).

4. Document the oldest operating systems that may be used and when it is not possible to utilize current operating systems and/or critical security patches, methods to secure the Workstation/device/equipment (e.g. network segmentation) shall be implemented.

5. Patch new equipment and software to the current patch level prior connecting it to any production network.

6. Develop a process and frequency to report the state of patching across all assets including the current status of all hardware device operating system levels and any missing patches.

d. When updated security patches are identified, the Information Technology Division and System Administrators shall:

1. Evaluate the patches to determine whether they adequately reduce risk or vulnerabilities and assign a patch rating as defined below:

Security Patch Rating	Definition	Action
Critical	Exploitation could result in compromise of the confidentiality, integrity or availability of restricted information assets or systems. Exposure is high on all platforms.	Patch or workaround should be applied immediately (unless it is documented that it will negatively impact systems / operations).
Important	Exploitation could result in compromise of the confidentiality, integrity or availability of information assets or systems, but to a lesser degree than a critical patch. Exposure to an exploit is mitigated by other factors.	Patch or workaround should be applied as soon as possible, no later than 1 week.
Moderate	Exploitation is mitigated to a significant degree by factors such as auditing, need for user action or difficulty of the exploitation.	Evaluate patch bulletin or workaround and apply as soon as possible, no later than 1 month.
Low	Exploitation is extremely difficult or there is minimal impact to information assets or systems.	Evaluate patch bulletin or workaround and apply in the course of normal maintenance operations if appropriate.

2. Make an analysis of patches to be deployed to determine system dependencies and outline a course of action to include testing and deployment

3. Work with contracted third-party vendors that manage Information Systems.

4. Test the patches:

   a). On test systems so any patch-related issues can be identified and resolved before the patches are installed on production systems (when available).

   b). To verify:

      1). They are effective in addressing the target vulnerability.

      2). They do not inadvertently cause other problems.

      3). Back-out or rollback options including data backup are available.

5. Deployment of patches:

   a). The Information Technology Division and System Administrators shall apply Workstation and software patch updates as they become available. This applies to all Workstations, including remote Workstations owned by the County. Examples include, but are not limited to:

      1). Windows operating systems

2). Smart phones

3). Java

4). Adobe, including Flash Player

5). Internet Explorer, Microsoft Edge, Google Chrome, etc.

6). Information Systems that create, receive, maintain, and / or transmit Confidential Information

b). The Information Technology Division and System Administrators shall deploy other appropriate patch updates as soon as possible following appropriate testing, and within two (2) weeks of their release, at a minimum, unless it is documented that it will negatively impact operations or systems.

6. Document implemented patches and decisions/reasons to reject security patches.

7. Also refer to the Firewall, Peripheral System Configuration, Router, Windows Server, Linux Server, Database, and Network Perimeter Management Design standards.

e. Auditing is completed on a monthly basis on a minimum of 5-10% of Information Systems, Workstations, Electronic Media, hardware devices, and other system components to verify patches are current and to check for zero critical updates.

5. Firewalls

a. Networks and servers are secured with secure stateful packet inspection Firewall(s).

b. The County firewalls may not be bypassed.

c. Refer to the Firewall Standard for baseline implementations.

Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Applicable Standards/Regulations

1. 45 CFR § 164.308(a)(5)(ii)(B) HIPAA Security Rule Protection from Malicious Software.

** NEW POLICY **

REMOTE ACCESS POLICY

Purpose

The purpose of this policy is to define and utilize uniform security requirements for remotely connecting to Chippewa County's (herein County) network and information assets. The requirements are designed to minimize potential exposure from damages that may result from unauthorized access to the County's information assets/systems and electronic protected health information (ePHI) and other Restricted Information as well as Sensitive Information.

Responsible for Implementation

The Security Officer and IT Division are responsible for implementing and overseeing this policy and procedures.

Policy

It is the policy of County to:

1. Safeguard electronic protected health information (ePHI) and other Restricted Information as well as Sensitive Information, collectively "Confidential Information" through established requirements for remote access to County 's networks and information systems.

2. Implement processes and mechanisms to support the confidentiality and safeguarding requirements as outlined in the Technology and Information Privacy and Security policy.

Procedures

1. Remote access is a privilege, and is granted only to remote users (e.g. management Workforce members and authorized contracted vendors) who have a defined need for such access and who demonstrate compliance with the County's established safeguards which protect the confidentiality, integrity, and availability of Confidential Information.

2. Access is approved as described in the System Access policy and Technology and Information Privacy and Security policy, when there is a clearly defined business need.

    a. Business associates, Subcontractors, contractors, and vendors may be granted remote access to the network, provided they have a contract or other required agreement with the County (refer to the Business Associate policies).

    b. The ability to print a document to a remote printer is not supported without approval by the IT Director.

3. Encryption:

    a. Security credentials are encrypted during transmission.

    b. Remote communication to the internal network over public networks is encrypted.

c. Workstations are encrypted, if Confidential Information is stored on them, as described in the Technical Access Control policy.

4. VPN access:

a. VPN gateway devices and configurations are set up and managed by the County's IT Division, users and their accounts are managed by the County.

b. Only the IT Division approved VPN connection originating from inside the County's network are allowed.

5. Remote host systems accessing the County's network must meet the County's security standards.

6. Personal equipment and workstations shall not be used to remotely access the County's network and/or information systems.

7. Only vendors authorized by the IT Division may use non-County equipment and workstations to remotely access the County's network and systems.

8. The County maintains logs of all activities performed by remote access users while connected to County's network (refer to the Auditing policy).

9. The IT Division shall facilitate remote access annual auditing of the security controls in place (for example 5-10% of remote access users should be audited of security user configurations annually).

10. The Security Officer and IT Division maintain documentation related to this policy and procedures for a minimum of six (6) years.

Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Resources

1. HIPAA COW Remote Access policy 2/27/13

Applicable Standards/Regulations

1. 45 CFR §164.312(a)(2)(iii) – HIPAA Security Rule Automatic Logoff
2. 45 CFR §164.308(a)(3)(ii)(B) – HIPAA Security Rule Workforce Clearance Procedures
3. 45 CFR §164.308(a)(3)(ii)(C) – HIPAA Security Rule Termination Procedures
4. 45 CFR §164.308(a)(4)(ii)(B-C) – HIPAA Security Rule Access Authorization

** NEW POLICY **

SYSTEM ACCESS POLICY

Purpose

To establish guidelines to protect Electronic Protected Health Information (ePHI), and other Restricted Information and Sensitive Information from unauthorized access, use, disclosure, and modification, as well as safeguards to prevent theft of Workstations and other equipment that create, receive, maintain, or transmit this information.

Responsible for Implementation

The Privacy Officer, Security Officer, IT Division, Human Resources Division, management team, and Department Heads are responsible for implementing and overseeing this policy and procedures.

Policy

It is the policy of Chippewa County (herein County):

1. To safeguard the confidentiality, integrity, and availability of Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other Restricted Information and Sensitive Information (collectively "Confidential Information") by controlling access to it.

2. To implement processes and mechanisms to support the confidentiality and safeguarding requirements as outlined in the Technology and Information Privacy and Security Policy.

3. To provide only the Minimum Necessary access to Confidential Information to all users, including but not limited to Workforce members, volunteers, business associates, contracted providers, consultants, and any other entities.

4. To prevent unauthorized access, use, disclosure, modification, and theft through established Workstation and Information System security safeguard controls.

Procedures

1. Roles: Role based access is provided to all Information System users, such as access to software, servers, Internet sites, transactions, Workstations, and portable devices that contain or transmit Confidential Information.

    a. Access levels for Information Systems are based on job classifications (based on business need, skill levels, and abilities to fulfill particular roles) and provide the Minimum Necessary access to Confidential Information needed to perform job responsibilities (treated on a least-access principle).

        1. Blanket access is not provided for any user.

2. Information Systems are programmed so that only the IT Division and other System Administrators are able to create and assign access to systems.

3. Individuals may not create their own access roles.

b. System Administrators and appropriate member of the management team / Department Head facilitate the following for all Information Systems and Workstations that create, receive, maintain or transmit Confidential Information, or otherwise provide access to Confidential Information:

1. Approve access levels/roles as well as requests for changes.

2. Maintain documentation describing the roles for all Information Systems and Workstations including the following:

a). Type of access such as read-only, modify, and full-access in different system functions

b). List of users assigned to each role (current and previous)

c). Analysis done to determine the access needs of users and the reasons for decisions made.

c. System Administrators, in collaboration with an appropriate member of the management team/Department Head annually when possible, but at a minimum every two years, shall provide the IT Director with a list of users with access to Confidential Information and review it to ensure they are consistent with authorized roles and continue to meet the Minimum Necessary access needed.

1. Changes are made, as appropriate to achieve Minimum Necessary access.

2. When roles are changed it is recommended that the reasons for the change as well as the date, time, and who changed it is documented and the documentation is maintained by System Administrators and appropriate member of the management team / Department Head.

2. Organizations, Consultants, and Vendors That Do Not Work Directly with Confidential Information: Have organizations, consultants and/or vendors that do not directly work with Confidential Information, that may inadvertently see and/or hear Confidential Information while working onsite, and a contract is not in place that otherwise requires protections of Confidential Information sign a Confidentiality Agreement for an Organization, Consultant and/or Vendor that Does Not Directly Work with Confidential Information.

3. Segregation of Duties: Access authorizations, changes, suspensions, and terminations are segregated to avoid conflict of interest, collusion, fraudulent or other malicious activity as it pertains to Confidential Information.

a. A single individual shall not perform a process from the beginning to the end without the involvement of another individual or group with appropriate authority. In smaller departments, segregation of duties is a challenge and it is recommended to request someone other than the individual who made the change to review the changes being made.

b. Users, regardless of their level of authority, shall not add or change their access without approval from an appropriate authority (e.g. user's Department Head or designee, system owner, Security Officer, Privacy Officer, etc.).

c. System administrators or any other user shall not change system security or audit functions without written approval from the Department Head or designee

4. Authorizing Access:

a. Background checks

1. Before individuals are allowed to access the organization's Information Systems, Workstations, portable devices, transactions, and servers, the Department Head or designee is required to provide the Human Resources Division with documentation of at least two positive work-related background checks prior to job offer and the Human Resources Division maintains documentation of the results.

2. Office of Inspector General (OIG) Exclusion List of Excluded Individuals and Entities (LEIE) are done upon hire and monthly by the Human Resources Division.

3. Caregiver Background checks are done upon hire and every four years by the Human Resources Division.

b. Access Requests

a. All users sign a "Confidentiality and Information Access Agreement" (Agreement), as well as other relevant privacy and security policies, procedures, and agreements. The Human Resources Division shall maintain a copy of the signed agreement.

b. For Third Party users, verify a Third-Party Agreement and/or Business Associate Agreement has been signed (refer to the Service Providers and Business Associate policies).

c. The appropriate Department Head coordinates efforts to request and approve access to department specific, managed, administered systems and maintain the following documentation (note: documentation is optional for Information Systems that do not create, receive, maintain, or transmit Confidential Information):

a). A copy of the request.

b). Name of the individual who requested the access.

c). Name of the person who set up the access.

d). The date and time access was set up.

e). User's assigned role(s).

d. The Department Head or designee shall complete a Request for Access (RFA) form to request access for users to Confidential Information (those listed on the RFA form):

a). Access levels and roles requested shall adhere to approved role-based access levels, as defined in the above Roles section.

b). For remote access requests, refer to the Remote Access Policy in the Information Technology Policy Manual for access permissions and safeguarding requirements.

c). Forward the completed RFA to the Human Resources Division at least two (2) weeks prior to the start date and the Human Resources Division shall forward the request to the IT Division.

e. The IT Division and other System Administrator(s) shall set up access based on the pre-approved roles. Emergency access may only be provided when normal processes cannot be conducted or are ineffective.

a). To request emergency access, a direct Supervisor or Department Head shall send an email to the IT Division. Include the following in the email:

1). Emergency situation.

2). Valid business purpose for access.

3). Unsuccessful normal access means attempted.

4). Who will be accessing the information.

5). For what period of time access will be granted.

6). The method of access.

b). Upon approval of the IT Division and the Department Head, emergency access may be provided.

c). Emergency access shall be immediately revoked when either the approved time period for access expires or the business purpose has been fulfilled.

f. The IT Division or other System Administrator(s) shall forward user names and temporary, unique, one-time use passwords directly to the user or Department Head in a secure manner (e.g. in a sealed envelope, call the user directly, send an internal email to the user, etc.).

g. The IT Division and other System Administrator(s) shall maintain the following documentation (note: documentation is optional for Information Systems that do not create, receive, maintain, or transmit Confidential Information):

a). A copy of the request.

b). Name of the individual who requested the access.

c). Name of the person who set up the access.

d). The date and time access was set up.

e). User's assigned role(s).

5. Modifying Access:

a. When a user's role changes or their access needs to an Information System, Workstation, portable device, transaction, or server is no longer needed, the Department Head shall:

1. Complete an RFA form and submit to the HR Division for Workforce members and contractors/vendors.

2. Coordinate efforts to change access to department specific, managed or administered systems and maintain the following documentation (note: documentation is optional for Information Systems that do not create, receive, maintain, or transmit Confidential Information):

a). A copy of the request.

b). Name of the individual who made the change request.

c.). The date and time access was changed.

d). Name of the person who changed the access.

e). Previous and new roles assigned.

3. Review the Facility Access policy for any additional requirements.

b. The HR Division shall forward the approved request to the IT Division (refer to the Authorize section above) to change the user's access role.

c. The IT Division / System Administrator(s) shall change the user's access after receiving the request, based on the pre-approved roles.

d. IT Division and System Administrator(s) shall maintain the following documentation (note: documentation is optional for Information Systems that do not create, receive, maintain, or transmit Confidential Information):

1. A copy of the request.

2. Name of the individual who made the change request.

3. The date and time access was changed.

4. Name of the person who changed the access.

5. Previous and new roles assigned.

6. Terminating Access:

a. When a user's access to the organization's Information Systems, Workstations, portable devices, transactions, and servers, is no longer required due to termination of the relationship with the organization, end of a specific project, or access is otherwise no longer needed, the Department Head shall:

1. Immediately, or as soon as practical, coordinate efforts to terminate access to department specific, managed and administered systems and maintain the following documentation (note: documentation is optional for Information Systems that do not create, receive, maintain, or transmit Confidential Information):

a). The date and time access was terminated.

b). Name of the person who terminated the access.

2. Collect equipment and other items distributed or owned by the County.

3. Email the Human Resources Division immediately, or as soon as practical, to notify them that the access shall be terminated. The Human Resources Division shall:

a). Request send an IT Help Desk ticket via email to deactivate the user's access.

b). Facilitate completion of the applicable Separation Checklist as a guide to make all necessary changes.

3. Review the Facility Access policy for any additional requirements.

b. Access shall be terminated if there is evidence or reason to believe the following (these shall also be reported on a Privacy and Security Incident Response form per the Incidents Policy):

1. The user has been using their access rights inappropriately.

2. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password).

3. An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).

c. The HR Division maintains a copy of the Separation Checklist (or documentation of the termination request received) and the reason for the termination.

d. The IT Division and other System Administrator(s) shall:

1. Terminate access immediately after receiving the request, but no later than 24 hours from the notification of the request, whether received verbally or in writing.

2. Maintain the following documentation regarding terminations (note: documentation is optional for Information Systems that do not create, receive, maintain, or transmit Confidential Information):

a). The date and time access was terminated.

b). Name of the person who terminated the access.

7. Logging-off Systems:

a. Information Systems that create, receive, maintain or transmit, or otherwise provide access to Confidential Information; VPN, Citrix, & other software application sessions; and Workstations are configured to automatically lock after a specified amount of inactivity as outlined in the Technology and Information Privacy and Security policy.

1. These timeframes are set by the IT Division and other System Administrator(s) and shall not be changed by users.

2. The user's password shall be used to re-establish the session.

b. Invalid attempt automated account locks for Information Systems that create, receive, maintain or transmit, or otherwise provide access to Confidential Information and Workstations settings are configured by the IT Division and other System Administrator(s), as outlined in the Technology and Information Privacy and Security policy.

8. User Authentication and Passwords:

a. Access to Information Systems and County's Confidential Information is controlled, at a minimum, by requiring a unique UN & PW for each individual user, including Administrator roles, so that access may be tracked.

b. Password safeguards

1. Vendor supplied default passwords shall be changed before a system is attached to County's network.

2. County leaders and System Administrators shall not maintain a list of user passwords, except for generic Workstation passwords (when authorized as stated above).

c. The IT Division and other System Administrator(s) shall set minimum password configurations as outlined in the Technology and Information Privacy and Security Policy and the Unique User IDs, Passwords, and Configurations Policy to the extent technologically possible, so that users are forced to use them.

9. Exceptions: Exceptions to this policy and procedures shall be authorized and documented by the Security Officer.

10. Documentation: All documentation related to this policy and procedures is maintained for a minimum of six (6) years from the date of creation or date it was last in effect, whichever is later.

11. Health Care Clearinghouse: This organization is not a health care clearinghouse, and therefore, does not have nor need any health care clearinghouse procedures.

Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Resources

1. HIPAA COW System Access Policy, Version 10, 4/4/05
2. OIG exclusion list:
   - Exclusion search: http://exclusions.oig.hhs.gov/
   - Downloadable database: http://oig.hhs.gov/exclusions/exclusions_list.asp
3. SAM database: https://www.sam.gov/portal/SAM/#1

Applicable Standards/Regulations

1. 45 CFR §164.308(a)(3)(i) HIPAA Security Rule Workforce Security
2. 45 CFR §164.308(a)(3)(ii)(B) HIPAA Security Rule Workforce Clearance Procedures
3. 45 CFR §164.308(a)(3)(ii)(C) HIPAA Security Rule Termination Procedures
4. 45 CFR §164.308(a)(4)(i) HIPAA Security Rule Information Access Management
5. 45 CFR §164.308(a)(4)(ii)(A) HIPAA Security Rule Isolating Healthcare Clearinghouse Function
6. 45 CFR §164.308(a)(4)(ii)(B) HIPAA Security Rule Access Authorization
7. 45 CFR §164.308(a)(4)(ii)(C) HIPAA Security Rule Access Establishment and Modification

8. 45 CFR §164.308(a)(5)(ii)(D) HIPAA Security Rule Password Management
9. 45 CFR §164.310(b) HIPAA Security Rule Workstation Use
10. 45 CFR §164.310(c) HIPAA Security Rule Workstation Security
11. 45 CFR §164.312(a)(1) HIPAA Security Rule Access Control (Technical)
12. 45 CFR §164.312(a)(2)(i) HIPAA Security Rule Unique User Identification
13. 45 CFR §164.312(a)(2)(iii) HIPAA Security Rule Automatic Logoff
14. 45 CFR §164.312(d) HIPAA Security Rule Person or Entity Authentication

** NEW POLICY **

BUSINESS ASSOCIATE POLICY

Purpose

To establish guidelines for Chippewa County (herein County) to identify vendor/business relationships which meet the HIPAA definition of a Business Associate and Subcontractor, provide direction in establishing formalized Business Associate Agreements (BAAs), and meet the requirements of the relationship between County and its Business Associates (BAs).

Responsible for Implementation

The Chippewa County Corporation Counsel, Privacy Officer, Security Officer, and Department Heads are responsible for implementing and overseeing this policy and procedures.

Policy

It is the policy of County to implement the required BA contract procedures and ensure documentation to establish satisfactory assurance of compliance with the HIPAA Privacy and Security Rules. It is the policy to have BAAs in place with BAs which establish appropriate safeguards for them to have in place for Protected Health Information (PHI) and Electronic Protected Health Information (ePHI).

Procedures

1. As indicated in the Vendor / Contractor Services section of the Information Privacy and Security policy, contact Corporation Counsel to assess whether a BAA is needed before entering into any agreement, contract, or other business relationship with any vendor or contractor, and before using, disclosing, or allowing them to create, receive, maintain, or transmit PHI or ePHI.

2. Corporation Counsel assesses whether a BAA is required, based on the:

    a. HIPAA definition of a BA

    b. The BA criteria provided in the BA definition in this policy

    c. Examples of Business Associates and Subcontractors Arrangements detailed later in the policy under Examples

    d. Examples of arrangements that are not Business Associates Relationships detailed later in the policy under Examples

3. When it has been determined that a BA arrangement exists with a vendor or contractor, Corporation Counsel or the Department Head or their designee shall facilitate getting a signed BAA document.

a. A BAA signed by Corporation Counsel or the Department Head or their designee shall be obtained before allowing the BA to acquire, access, use, or disclose protected health information or electronic protected health information (ePHI)

b. Every attempt possible should be made to utilize County's BAA template

c. If a vendor or contractor relationship requiring a BAA is in the process of contract negotiation and development, the provisions of the BAA may be incorporated into the contract, or provided as a separate document

d. The following information shall be entered into County's BAA template, before providing it to the vendor or contractor:

1. Permitted uses and disclosures of PHI as applicable to the arrangement, if different than those stated in the BAA template.

2. Limitations on the use and disclosure of PHI as applicable to the arrangement, if different than those stated in the BAA template.

3. The name and address of the BA, as well as the name of the individual that will sign it.

4. When County hires or contracts with an individual or organization, the BAA with that BA includes the same (or more stringent, as applicable) restrictions and conditions as in the BAA with the originating organization

5. County does not have nor need any procedures to meet any governmental BA requirements.

4. Negotiating and/or signing of a different organization's BAA.

a. Examples of negotiating and/or signing a different organization's BAA:

1. The County may serve as a BA to another organization and may be asked to review and sign that organization's BAA.

2. A vendor or contractor may request changes be made to County's BAA.

3. After several attempts, a vendor or contractor may refuse to sign the County's BAA and require the County to sign their BAA.

b. In these situations, Corporation Counsel reviews the submitted BAA to ensure that the provisions outlined are consistent with those set forth in this policy as well as the County's BAA template, and contains all the required Privacy and Security Rule BA contract provisions. If the BAA is not consistent with this policy, the County's BAA, and/or contains additional provisions or provisions that are inconsistent with the regulations, Corporation Counsel may proceed with the following alternatives:

1. Agree to the additional or different provisions and sign the BAA, if the inconsistencies are legal and acceptable.

2. Refuse to agree to the provisions and work with the other organization to establish a resolution.

5. When the provisions of the County's BAA change (due to legal or organizational changes), Corporation Counsel, the Department Head or their designee shall facilitate getting either a new BAA or BAA Addendum signed by all of the County's BAs.

6. The County does not have a statutory obligation to continuously monitor the activities of its BAs. The IT Division or Security Officer, however, facilitates the following:

a. Before entering into any agreement, contract, or other business relationship with any vendor or contractor, and before disclosing and allowing them to create, receive, maintain, or transmit Confidential Information refer to the Service Provider policy for additional steps to take.

b. Respond to reported privacy and security violations and breaches of unsecured PHI reported by the BA.

1. Works with the BA to take reasonable steps to cure any potential violation or end the violation.

2. Requests the BA provide information as to how and why the violation happened, all breach notification elements (as required in the Incidents Policy), measures they are taking to cure the violation and prevent it from reoccurring, and verification that appropriate disciplinary actions were provided to the violating party(s).

3. If the County knows of a pattern of activity or practice of a BA that constituted a material breach or violation of the BA's obligation under the BAA and steps taken to cure the cure the breach or end the violation were unsuccessful, terminates the BAA, whenever feasible. If not feasible, documents the reasons it is not feasible to terminate the BAA.

c. If any County workforce member becomes aware of a potential problem with the BAA, notify the Privacy Officer and/or Security Officer.

1. The Privacy Officer and/or Security Officer or designee notifies any other County workforce who may be able to assist with the situation, and takes reasonable steps to correct the problem.

2. The Privacy Officer and/or Security Officer or designee contacts the BA as soon as possible after discovering the potential infraction to address the issue. Depending on the terms of the BAA with the BA, the County will assess the options for termination or allowing a cure period.

7. The County is not a BA of another organization; therefore, it is does not have nor need any procedures to follow any other organization's BAA.

8. BAAs are effective for the length of the relationship between the BA and the County, unless otherwise terminated under the provisions outlined in the BAA.

9. When a BA contract terminates, Corporation Counsel, the Department Head or their designee shall request the BA to return, destroy, dispose or sanitize all PHI and/or ePHI, according to the Disposal of Confidential Information Policy.

    a. If the BA destroys, disposes or sanitizes the PHI and/or ePHI, obtain written notification from the BA this was done.

    b. If returning, destroying, disposing or sanitizing is not feasible, request the BA to provide written notification that they agree to limit the use and disclosure of the information and documentation of the reason that is preventing the PHI and/or ePHI's return, destruction, disposal or sanitization.

10. Corporation Counsel, the Department Head or their designee shall maintain the following BAA documentation for a period of six years beyond the date of when the BAA relationship is terminated:

    a. Copy of the fully executed (signed) BAA in a place where it can be easily retrieved

    b. Name of the BAA

    c. Term of the contract

    d. Any additional notes, such as negotiations, as appropriate

Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Examples

EXAMPLES OF BUSINESS ASSOCIATES AND SUBCONTRACTOR ARRANGEMENTS INVOLVING PHI THAT REQUIRE A BUSINESS ASSOCIATE AGREEMENTS OR CONTRACT PROVISIONS	
Accrediting/Licensing Agencies (JCAHO) Accounting Consultants/Vendors Actuarial Consultants/Vendors Administrative Services Agents/Contractors Accessing PHI (Consultants) Application Service Providers (i.e., prescription mgmt.) Attorneys/Legal Counsel Auditors Backup service provider Benchmarking Organizations Benefit Management Organizations Billing Claims Processing or Administration / Clearinghouse Agency Contracts Cloud hosting vendor Coding Vendor Contracts Collection Agency Contracts Computer Hardware Contracts Computer Software Contracts Consultants/Consulting Firms Data Aggregation Data Analysis, Processing, or Administration Consultants/Vendors Data Storage Company Data Transmission Services that requires routine access to PHI Data Warehouse Contracts E-prescribing Gateway Emergency Physician Services Contracts Financial Services Health Information Organization (HIO) Hospitalist Contracts Insurance Contracts (Coverage for Risk, Malpractice, etc.) Interpreter Services Contracts IT/IS Vendors Legal Services Contracts Management Medical Staff Credentialing Software Contracts Microfilming Vendor Contracts Optical Disc Conversion Contracts	Pathology Services Contracts Paper Recycling Contracts Patient Safety Activities listed at 42 CFR 3.20 Patient Satisfaction Survey Contracts Payer-Provider Contracts (Provider for Health Plan) Personal Health Record Vendor (provided on behalf of the Organization to individuals) Physician Billing Services Physician Contracts Practice Management Consultants/Vendors Professional Services Contracts Quality Assurance Consultants/Vendors Radiology Services Contracts Record Copying Service Vendor Contracts Record Storage Vendors Release of Information Service Vendor Contracts Repair Contractors of Devices Containing PHI (digital copy machines, hardware, etc.) Repricing Researcher (performs a function, activity, or service for a CE that falls within the definition of BA; note that this is a limited scope; as Research is not a business associate service (does not fall under the definition of a business associate) Revenue Enhancement/DRG Optimization Contracts Risk Management Consulting Vendor Contracts Shared Service/Joint Venture Contracts with Other Healthcare Organizations Statement Outsource Vendors Telemedicine Program contracts Third Party Administrators Transcription Vendor Contracts Utilization Review Waste Disposal Contracts (Hauling, Shredding) <u>Health Plan Relationships:</u> Pharmaceutical Benefits Management Contracts Preauthorization Management Contracts Case Management Contracts Third Party Administrator (TPA) Contracts Wellness Promotion Contracts

EXAMPLES OF ARRANGEMENTS THAT ARE NOT BUSINESS ASSOCIATE RELATIONSHIPS AND DO NOT REQUIRE BUSINESS ASSOCIATE AGREEMENTS OR CONTRACT PROVISIONS	
Banks Processing Credit Card Payments Blood Bank/Red Cross (Provider) Clinics (Provider Relationships) Courier Services Delivering Specimens Device Manufacturers Require PHI to Produce Pacemakers, hearing aids, glasses, etc. (Treatment) Cleaning/Janitorial Services (if do not handle PHI) DME for Equipment for Treatment Purposes Educational/School Programs (Student Privacy Education Required as Workforce Member) Health Plans Contracting With Network Providers (Covered Entity to Covered Entity) Health Plans for Purposes of Payment Hospitals Housekeeping/Environmental Services (Incidental Exp.) Infusion Provider for Treatment Institutional Review Board Internet Service Providers (ISPs) providing mere data transmission services Law Enforcement Agencies Members of an Affiliated Covered Entity Members of the Organization's Organized Health Care Arrangement (OHCA) Pharmacy (Healthcare Provider/Treatment) Providers (Involved in Care & Treatment of Patient)	Members of the Organization's Workforce Organ Procurement Organizations Nursing Homes (for treatment and payment) Quality Improvement Organization –Agent of CMS (MetaStar) Rental Employee Agencies (if no PHI Shared – Employees Need Privacy Training) Repair Contractors (Maintenance) Researcher Conducting Research Activities Plumbing, Electricity, etc. – (if no PHI involved) School Health Nurses Supply Services Support Services Agreements for Supplies/Tx Purposes Tissue Banks Telecommunications company with occasional, random access to PHI U.S. Post Office and Other Couriers Volunteers (Board Members, Ethics Committee Members, IRB Members, etc.) Note: a CE is not required to have a BAA with a BA's Subcontractor (the BA is required to have a BAA with their Subcontractor)

Applicable Standards/Regulations

HIPAA Final Omnibus Rule, January 25, 2013
45 CFR § 164.308(b)(1-3) HIPAA Security Rule Business Associate Contracts and Other Arrangements
45 CFR §164.314(a)(1) HIPAA Security Rule Business Associate Contracts or Other Arrangements
45 CFR § 164.314(a)(2)(i) HIPAA Security Rule Business Associate Contracts
45 CFR § 164.314(a)(2)(ii) HIPAA Security Rule Other Arrangements
45 CFR § 164.314(a)(2)(iii) Business Associate Contracts with Subcontractors
45 CFR § 164.502(e)(1) HIPAA Privacy Rule Disclosures to Business Associates
45 CFR §164.504(e) HIPAA Privacy Rule Business Associate Contracts

** NEW POLICY **

CONTINGENCY PLAN POLICY

Purpose

The purpose of this policy is to protect people, property, and data during emergencies and to provide procedures to recover operations should an emergency or Disaster render any part of Chippewa County's (herein County) electronic protected health information (ePHI), and other Restricted Information, and Sensitive Information, collectively "Confidential Information" unusable. It works in conjunction with any County Continuity of Operations Plans (COOPs). The policy helps to provide assurances that the County has the capabilities necessary to respond to emergency and Disaster situations and support the continuity of business operations is accomplished by:

- Establishing secure and resilient information technology and operational process environments.
- Documenting information technology contingency and continuity of operations plans and having them readily available when needed.
- Assigning roles and responsibilities within the plans.

The policy will assist and allow for services to continue during an interruption and limit the impact of the negative effects that disruptions could have on the organization's reputation, critical operations, liquidity, credit quality, internal and external communications, and ability to remain in compliance with applicable laws and regulations.

Goals

1. Provide reference plans to protect the safety and security of workforce members, property, and data during emergency situations.
2. Limit the amount of time information systems may be inaccessible by establishing:
    a. Comprehensive plans
    b. Authorities
    c. Responsibilities
    d. Secure and resilience tested IT and operational process environments
3. Anticipate worst-case threat sources, emergency situation, and/or Disaster scenarios and:
    a. Determine what could happen if the organization's Confidential Information (or other significant portions of an organization's infrastructure external or internal to the organization) is partially or totally destroyed or otherwise unavailable.
        1. Understand criticality and dependencies between business and operational processes and IT infrastructure, systems, and service providers.

2. Formally set and approve data criticality and/or Recovery Time and Recovery Point Objectives (RTO/RPO) as well as any identified gaps.

3. Address approved internal and service provider gaps.

b. Decide and document measures describing how best to react to them and recover information systems.

c. Continue to ensure the confidentiality, integrity, and availability of Confidential Information during the situation and while recovering from it; and

d. Have documented COOPs available when they are needed.

4. Facilitate the prompt resumption of critical services.

5. Establish requirements for periodic testing of the adequacy of the plans.

6. Provide guidelines to update plans with operational and environmental changes.

7. Provide training to stakeholders at and workforce members as appropriate to ensure business continuity and information security during emergency events.

Responsible for Implementation

The IT Director oversees and has the authority and overall responsibility for facilitating the implementation, activation, coordination, and documentation of IT Contingency Plan, IT ISCP, this policy, and IT related Disaster recovery operations.

The IT Director, Privacy Officer, Security Officer, Emergency Management Director, and IT Division are responsible for establishing, implementing, and overseeing emergency and disaster action plans, and COOPs for the IT Division. They are also responsible for working with each department as applicable and needed for the emergency situation.

The IT Director is responsible for ensuring that the policies, procedures, and IT ISCP are compatible and are simultaneously updated when significant changes occur as they pertain to IT and security related practices.

The IT Division, Department Heads, and System Administrators are expected to be familiar with the policies, Contingency Plans, and COOPs, in place. They are also expected to participate as assigned in disaster recovery testing.

Refer to the IT Policy Manual's Technology and Information Privacy and Security policy – Contingency Plan section for general Workforce member requirements.

Policy

It is the policy of Chippewa County:

1. To have systems, especially those containing Confidential Information, available at all times as well as during an emergency or a Disaster as needed and feasible to provide critical business functions as defined in the COOPs.

2. To provide the organization with a current and approved information system Contingency Plan and IT ISCP that support protection of workforce, timely restoration, and recovery of interrupted critical clinical and business operations during an emergency or Disaster situation.

3. To minimize possible adverse clinical outcomes, as well as financial and business impacts, to the organization as a result of an interruption of normal business operations through established manual and automated methods of accessing needed information during an emergency.

4. To meet the needs of the organization's clients, consumers, subscribers, Workforce members, customers, and other stakeholders reliant on the organization's ability to provide necessary services during and following an emergency or Disaster situation.

5. To continue to protect Confidential Information to the extent possible even during emergencies and Disasters.

6. To protect the public image and credibility of the organization.

7. To have business interruption insurance.

Procedures

1. Disaster Recovery Planning

    a. Appropriate resources are allocated based on IT initiatives, planned exercises, and other COOP needs.

    b. To limit the impact of emergency situations and Disasters, all reasonable efforts are made to have security controls and contingency plans and IT ISCP in place that minimize the amount of time systems may be down to the least possible, but no more than documented recovery time objectives for critical systems as long as it does not unduly hinder operational performance, jeopardize security, or increase costs.

2. Environmental Controls

    a. Critical Confidential Information systems are on a UPS and a generator and:

        1. They are tested semi-annually by contracted service providers.

        2. The Facilities and Parks Division inspects them quarterly at a minimum.

        3. The UPS powers this equipment long enough for the generator to start providing power.

    b. The following are in the server room:

        1. A cooling system

2. A backup cooling system

3. Fire suppression system

4. Electrical fire rated fire extinguisher

5. Temperature and fire alarms/paging

6. All of the above are:

a). Located away from any water and sewage source.

b). Locked room with access limited to the minimum necessary to maintain or recover systems; access audit trails are maintained.

c). Have emergency lighting in the event of a power outage or disruption meets the "Life Safety Code" and "National Electric Code".

a. The following are in each data wiring room/closet:

1. Electrical fire rated fire extinguisher (in or near the rooms).

2. Locked room with access limited to the minimum necessary to maintain or recover systems.

b. The following are available at each critical facility:

1. Backup internet service.

2. Generators with a large onsite storage of backup fuel.

c. All reasonable efforts are made to ensure Business Associate providers that create, receive, maintain, transmit, and backup Confidential Information have sound environmental security controls that minimize downtimes and allow them to recover systems within identified recovery times, such as the above stated controls.

3. Contingency Plans

The IT ISCP includes, at a minimum, the following:

a. A list of most significant types of Threat sources that are the most likely to damage systems containing or affecting the availability of Confidential Information and/or critical systems. Refer to the Information Security Risk Management policy for additional threat source identification requirements.

1. List environmental, human, natural, technology, and other types of Threat sources to the organization's people, facilities, and IT infrastructure.

2. Prioritize Threat sources based on their likelihood of occurring and severity levels (e.g. impact on operations).

3. Identify operational vulnerabilities and weak business processes.

4. Determine cost-effective mitigation strategies to reduce the Threat likelihood or impact.

b. Procedures to respond to different types of Threat sources and emergency situations or Disasters for each significant area of the IT Division.

1. The primary consideration in any situation is the safety of all workforce members, customers, clients, consumers, and vendors. Steps outlined in the IT ISCP include:

a). How to protect the safety of all individuals and safely evacuate the facility(s).

b). Who is responsible for evacuating the facility(s) and the server room.

2. How quickly to use technical resources after a Disaster occurs.

3. Incorporate Contingency Plans or disaster recovery plans from vendors and other Business Associates when they are necessary to be included in the County's contingency plans and/or COOPs.

4. Procedures outlining how to backup and recover each Confidential Information system and critical information technology operations (also refer to the Data Backup and Media Management policy and procedures).

a). For each system affected, procedures include a "return to operations" transition plan to execute to move data into the production or emergency operational environment.

5. Procedures to restore lost Confidential Information for each type of system which stores Confidential Information, including what data to restore.

6. To provide client and consumer care and other critical services, procedures include arrangements for a Recovery Facility(s) for the IT Disaster recovery command center, as needed.

a). The command center functions as the centralized location for IT Disaster recovery processes and has the necessary critical resources and equipment required for Disaster recovery.

b). Recovery Facility locations include:

1). Telephone system: Highway Department building.

2). Redundant data center: contract agreement with City of Eau Claire.

3). 911 failover site: contract agreement with Dunn County.

c). Documentation includes the steps and resources needed to bring the Recovery Facility locations on-line while maintaining the security of Confidential Information.

7. Identification of facility security controls, including the following:

a). Only the following individuals (that are able to assist in restoring access to Confidential Information) may have access to and be in the server and data wiring rooms as well as have access to backups, even during emergencies and Disaster situations:

1). IT Division

2). Facilities and Parks Division

3). Individuals authorized by the IT Division and/or and Facilities and Parks Division

b). In the event of an emergency situation that renders the server and data wiring rooms uninhabitable (e.g. fire, chemical spill, tornado, etc.), appropriate emergency personnel will control access to the site during the entire course of the emergency.

1). Priority will be given to the safety of people and to evacuating as much equipment as possible to a safe indoor location, or a safe and guarded outdoor location, until it can be moved to a better location. If necessary, on site IT Division and/or and Facilities and Parks Division workforce will direct the effort and work with other agencies to secure help to move and transport equipment.

2). Movement, repair, and restoring of service will be prioritized. Equipment will be secured in accordance with the level of security of the information that remains.

c). Authorized individuals also have electronic device access and/or keys to enter Recovery Facility locations to assist in efforts to restore access to Confidential Information.

d). During emergencies:

1). The Emergency Management Department evaluates whether a location needs to be closed or secured with security guards to assist in efforts to secure it.

2). Workforce may not attempt to enter any location that is blocked off by security or emergency crews, unless authorized

by the IT Director, Privacy Officer, Security Officer, Emergency Management Director, or IT Division.

c. A contact list for each system (refer to the Vendor Emergency Contact Information form).

1. The contact list includes key workforce members and their designated alternates, key vendors, and other individuals that help support and recover systems such as: data center personnel, system administrators; IT network, infrastructure, and systems management; workstation management; storage management; help desk team; Business Associates; service providers (including service provider dependencies)**;** stakeholders; utilities management (e.g. electric, water, gas); telecommunications/phone; internet services provider(s); emergency government and law enforcement/government agencies.

2. The contact information for each includes name(s), company name(s), address, main and backup telephone numbers, email address, and web site address, as applicable.

d. A current Inventory Asset List for each system, application, server, hardware, IS equipment (workstations, portable devices, etc.), network information/specifications, etc. purchased or leased by County that are used to access, create, receive, maintain, or transmit Confidential Information. This list includes, at a minimum and as applicable:

1. Type of asset with model and serial numbers, manufacturer, operating systems, warranty information, etc. so items can easily be replaced, as applicable.

2. Critical functions which help determine how important each system is to business needs.

3. Documentation required for recovery.

4. Indication of the critical systems that are supported at alternate sites.

5. Location (physical or logical) and who uses each Confidential Information system, workstation, and portable device.

6. Interdependencies/interoperability on other systems, applications, servers, etc., with a recovery plan for each.

7. Data owner.

8. Whether Confidential Information is created, received, maintained, or transmitted by the asset.

9. The identification tag number of fixed assets with a value over $5,000.

10. Expected date of retirement.

11. Retired assets.

12. Assign a Data Criticality Level for each system, application, server, hardware, IS equipment, network information/specifications, etc. This may be done in a variety of ways, such as assigning a data criticality level and determining the recovery point objective (RPO) and recovery time objective (RTO) for each.

    a). Software applications and data points that create, receive, maintain, or transmit Confidential Information are included on the list (refer to the Systems Matrix). Financial and operational considerations, as well as regulatory requirements and legal obligations may also be a part of this consideration.

    b). Applications, systems, and/or networks that need to be available at all times and need to be recovered/restored first are prioritized; they are ranked in order of critical functions and recovery order.

e. A current network diagram.

f. Copies of site maps, building plans, and insurance policies.

g. A list of Disaster recovery supplies needed and ensures that they are readily available (refer to the Disaster Recovery Supply Checklist).

h. Detailed downtime procedures (developed by each Division or Department) outline how to continue providing services during an emergency situation in a secure manner to the extent possible.

i. Approval of the plans as well as any identified gaps by the County Administrator or designee.

4. Emergencies: Activation of the Contingency Plan and Disaster Recovery Plan

a. Contact the IT Division when a system(s) and/or network is down.

b. Refer to the ISCP for next steps and notifications that are made by designated personnel.

c. During emergencies, all users must continue to protect Confidential Information to the extent possible, to prevent a breach of confidentiality.

d. System Recovery:

    1). The IT Division shall recover information systems and bring them back into operations as outlined in the recovery downtime and procedures. In situations that affect only single systems, the IT Division determines the appropriate response, implements it, and restores the system.

    2). Use a Privacy and Security Incident Response form when systems are down and meet the definition of a Security Incident (refer to the Incidents policy).

5. Contingency Plan Testing and Maintenance

a. Testing

1. Contingency Plan and/or IT ISCP testing shall be done to evaluate the effectiveness of the Contingency Plan as well as feasibility of the recovery strategies, and improve it based on outcomes.

2. Contingency Plan and/or IT ISCP testing is done on an annual basis, when possible, but shall be at a minimum every two (2) years. Notifications are provided to users of potentially affected systems prior to testing being conducted, as appropriate.

a). A scenario-based walk-through or "mock" drill is done to examine the plans and determine the need for changes.

b). Testing includes some or all of the following:

1). The ability to access alternative computers and/or sites in a timely manner.

2). Loading and running any necessary programs.

3). Loading, reviewing, and using Confidential Information.

4). The ability to access Confidential Information in order to contact individuals, as necessary.

c). When full recovery tests are done, they simulate an actual emergency or disaster situation.

d). Backup sites are also reviewed to verify they support Contingency Plan and/or IT ISCP needs (with backed-up Confidential Information), should the main facility be compromised.

3. During the normal use of any system, components fail. Document why the system was down and how the system was recovered. Maintain this documentation as a part of the Contingency Plan and/or IT ISCP testing files.

b. Maintenance and Revision

1. The IT Director is responsible for maintenance and revision of the Contingency Plans and/or IT ISCPs.

a). The Contingency Plans and/or IT ISCPs shall be reviewed and revised a minimum of every two (2) years, and when needed to ensure that the information it contains is current.

b). The Contingency Plans and/or IT ISCPs are reviewed and revised to address issues identified after a planned test and actual Disaster.

2. All revisions shall be provided to those that need to follow the plans.

6. Education and Training

a. Users of critical systems are trained on how to access necessary Confidential Information during an emergency and continue to protect Confidential Information during emergencies, as applicable to their roles.

b. Workforce members are provided education and training in emergency preparedness and the contingency plans upon hire, annually, and when significant changes to the organization's contingency plans, emergency preparedness, and Disaster recovery plans are made that impact them.

c. Workforce members with specific responsibilities for IT Disaster recovery shall receive specific training so that they can carry out their assigned duties.

d. Other stakeholders are provided training as appropriate to ensure business continuity and information security during emergency events.

7. Documentation

a. Copies of the Contingency Plan and Disaster Recovery Plans are maintained on and offsite and are readily available in the event of an emergency.

1). Copies are maintained within a shared drive to which all key individuals have access. This shared drive is automatically backed up at the City of Eau Claire back up data center; this could be accessed via the Internet and/or physically during an emergency.

2). Copies are easily accessible to those individuals that need to activate the Disaster recovery plan and recover systems.

b. Contingency Plans and IT COOPs information, including the controls in place, testing, and revisions are maintained for six (6) years from the last date in effect.

8. Exceptions

a. Exceptions to this policy and procedures are authorized and documented as outlined in the Privacy and Security Oversight procedures.

Reporting and Compliance

Refer to the Information Privacy and Security policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Resources

1. NIST Contingency Planning Guide for Federal Information Systems, SP 800-34 Rev 1, November 2010
2. HIPAA COW Contingency Planning Whitepaper v8, 4/25/06
3. HIPAA COW Risk Analysis & Risk Management Toolkit 10/12
4. SANS Institute Disaster Recovery Plan Policy, 2014

Applicable Standards/Regulations

1. 45 CFR § 164.308(a)(7)(i) HIPAA Security Rule Contingency Plan
2. 45 CFR § 164.308(a)(7)(ii)(B) HIPAA Security Rule Disaster Recovery Plan
3. 45 CFR § 164.308(a)(7)(ii)(C) HIPAA Security Rule Emergency Mode Operation Plan
4. 45 CFR § 164.308(a)(7)(ii)(D) HIPAA Security Rule Testing and Revision Procedure
5. 45 CFR § 164.308(a)(7)(ii)(E) HIPAA Security Rule Applications and Data Criticality Analysis
6. 45 CFR § 164.310(a)(2)(i) HIPAA Security Rule Facility Access Controls/Contingency Operations
7. 45 CFR § 164.312(a)(2)(ii) HIPAA Security Rule Access Control/Emergency Access Procedure

** NEW POLICY **

DISPOSAL OF CONFIDENTIAL INFORMATION POLICY

Purpose

To define appropriate mechanisms to utilize before reusing Media and to dispose of all Media that contains Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other restricted and sensitive information (collectively "Confidential Information") so that this information is not inappropriately Accessed by or disclosed to unauthorized individuals or is erased or destroyed within Chippewa County's (herein County) retention guidelines.

Responsible for Implementation

The Privacy Officer, Security Officer, Facilities and Parks Division, and IT Division are responsible for implementing and overseeing this policy and procedures.

Policy

1. It is the policy of County to ensure the privacy and security of Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other restricted and sensitive information when it is no longer needed using secure disposal mechanisms.

2. When Media containing Confidential Information is going to be reused, to take appropriate steps to ensure that all stored Confidential Information is removed.

3. To destroy or dispose of Confidential Information when it is no longer being used and in accordance with Federal Regulations, applicable State laws, and as defined in the Retention Policy and Records Retention Chapter 3 of the Chippewa County Code of Ordinances.

4. To suspend the schedule for destruction or disposal for client, consumer, and subscriber records involved in any open investigation, audit, or litigation.

Disposal of Media

1. Refer to the Information Privacy and Security Policy or Disposal of Confidential Information Policy for general Workforce member and Business Associate (BA) responsibilities for collecting, identifying, segregating, and disposal of all types of Confidential Information on behalf of the organization.

2. All destruction, disposal or Sanitization of Confidential Information shall be done according to County client, consumer, and subscriber record retention policy and schedule (and as allowed by law).

3. Preservation or destruction or disposal of patient health records upon closure of a provider office or practice shall be done so by following Wisconsin Statute 146.819 which outlines the detailed procedures for the appropriate preservation or destruction or disposal of patient health records for a health care provider who ceases to practice. The provider, or the personal representative of a deceased health care provider, shall comply with the statutes to ensure appropriate preservation, patient notice, destruction and/or disposal of the patient health care

records in the possession of the health care provider at the time the practice was ceased or the provider died. This statute does not apply to:

a. Community-based residential facilities or nursing homes

b. Hospitals

c. Hospices

d. Home Health Agencies

4. The IT Division facilitates the following for Electronic Media:

a. Removal of all software licenses prior to disposal.

b. Securing Media containing Confidential Information that is scheduled for destruction, disposal or Sanitization to prevent unauthorized or inappropriate access until the destruction or disposal is complete.

c. After internally wiping or Sanitizing a disk or other electronic Media, placing a sticker or label on it that includes the date and name of the technician who performed the wipe.

5. When destruction, disposal or Sanitization services are contracted:

a. Contract with a National Association for Information Destruction (NAID) certified company.

b. For disposal of PHI and ePHI, a Business Associate Agreement is obtained which includes contract language specific to these services as required by the Business Associate Policy.

1. When a BA contract terminates, follow the Business Associate Policy for the proper return and or destruction of PHI and ePHI.

c. For disposal of all other Confidential Information, a contract including security policy requirements is obtained.

6. Documentation of Disposal:

a. The Facilities and Parks Division, IT Division, or their designee creates or obtains and maintains destruction, disposal or Sanitization documentation of Confidential Information:

1. This shall be done on a Certificate of Destruction form.

2. The form includes the following information:

a). Date of destruction, disposal or Sanitization;

b). Name and contact information of the individual or organization that performed the destruction;

c). Method of destruction, disposal or Sanitization;

d). Description of the destroyed, disposed or Sanitized record series or medium;

e). Inclusive dates covered;

f). A statement that the client, consumer or subscriber records were destroyed, disposed or Sanitized in the normal course of business; and

g). The signatures of the individuals supervising and witnessing the destruction disposal or Sanitization.

7. The IT Division updates the status of the inventory asset list, including all hardware and licensed software.

8. Confidential Information destroyed, disposed or Sanitized using a method that ensures the Confidential Information cannot be recovered or reconstructed. Methods used may include those detailed in the table the follows.

Media Disposal Methods

Medium	Examples of Method to Use
Audiotapes	• Recycle (tape over), Degauss, or pulverize.
Electronic data / hard disk drives including drives found in servers, Workstations, printers, copiers, fax machines, scanners, and network / communication devices (e.g. routers and firewalls)	When applicable, remove the device from the central management server; then: • Destroy data permanently and irreversibly through: ○ A Department of Defense (DoD) wipe (e.g. disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks) ○ Physical destruction (pulverize, shred, disintegrate, incinerate) ○ Degaussing of it, or ○ Hard drive erasure software • Methods of reuse: overwrite data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten.
Electronic data / removable media or devices including USB drives, SD cards, CDs, tapes, and cartridges	• Overwrite data with a series of characters or reformat it (destroying everything on it). Total data destruction does not occur until the data has been overwritten. • Magnetic Degaussing that leaves the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic Degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. • Shredding or pulverization is done for the final disposition of any removable Media when it is no longer usable.

Medium	Examples of Method to Use
Portable / handheld devices including cell phones, smart phones, PDAs, tablets, dictation and recording devices, cameras (still and video), barcode / smartcard readers, hand-held printing devices (e.g. labeler), media players, mapping/navigation devices, etc.	First, when applicable, remove the device from the central management server, then: • Activate the software on these devices that remotely wipes ("bit-wipe") data off the device. • Complete the following steps: ○ Manually delete all files/data, configuration/connection information, phone calls/texts sent/received, addresses/contact information, speed dial numbers, pictures, calendar entries, recordings, locations, email, documents, etc. ○ Perform a full manufacturer's reset back to the factory default settings • When a handheld device is no longer reusable it is then totally destroyed by recycling or by trash compacting
Labeled devices, containers, equipment, etc.	• Shred or destroy so that the Confidential Information cannot be read or otherwise cannot be reconstructed; redaction is specifically excluded as a means of data destruction • Reasonable steps should be taken to destroy or de-identify any Confidential Information prior to disposal of this medium. Remove labels or incinerate the medium; or • Ribbons used to print labels may contain Confidential Information and are shredded or incinerated.
Microfilm/ Microfiche and X-rays	• Shred or destroy so that the Confidential Information cannot be read or otherwise cannot be reconstructed; redaction is specifically excluded as a means of data destruction • Recycle through a contracted BA or burn/pulverize it.
Optical media	• Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Paper records	• Refer to the Information Privacy and Security Policy – Disposal of Confidential Information procedures for disposal requirements.
Videotapes	• Recycle (tape over) or pulverize.

Reuse of Electronic Media Containing Confidential Information

1. Before the reuse of any recordable and erasable Media (e.g. hard disks, workstations, laptops, tapes, cartridges, USB drives, smart phones, SAN disks, SD and similar cards), the IT Division facilitates removal of all Confidential Information and/or makes it inaccessible, cleaned, or scrubbed through one of the following methods:

   a. <u>Reused within the organization:</u>

      1. Overwrite the data (for example, through software utilities);

      2. Degauss the Media; or

      3. Reformat it so that files are not accessible to the new user(s).

   b. <u>Reused external to the organization</u> (e.g. sell or donate the media): destroy, dispose or Sanitize the media according to the Electronic Data or Hard Disk Drives method described above.

2. The IT Division or designee:

a. Documents and/or obtains documentation when this is done, as well as the method used to remove information and date/time it was completed

b. Updates the inventory asset list with all hardware and licensed software.

3. The Privacy officer, Security Officer, Facilities and Parks Division, and IT Division periodically reviews and updates the methods of destruction, disposal or Sanitization and reuse, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal or Sanitization and reuse technologies and services.

4. All documentation is maintained for a period of six years after the destruction, disposal or Sanitization was completed.

Reporting and Compliance

Refer to the Information Privacy and Security policy for requirements to report suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms, refer to the HIPAA Privacy and Security Definitions form located on the Employee Portal under Policies / Department of Administration.

Resources

- SANS Technology Equipment Disposal Policy, June 2014
- HIPAA COW Device, Media, and Paper Record Sanitization for Disposal or Reuse Policy, Revised 10/8/12

Applicable Standards/Regulations

- 45 CFR § 160.103(a) HIPAA definition of Electronic Media (1/25/13)
- 45 CFR §164.310(d)(1) HIPAA Security Rule Device and Media Controls
- 45 CFR §164.310(d)(2)(i) HIPAA Security Rule Disposal
- 45 CFR §164.310(d)(2)(ii) HIPAA Security Rule Media Re-use
- 45 CFR §164.504 (f)(2)(ii)(I) HIPAA Privacy Rule Requirements for Group Health Plans
- Sec. 895.505 Wis. Stats. Disposal of records containing personal information, including medical records
- Sec. 146.819 Wis. Stats. Disposition of patient health records for a provider who ceases to practice
- Wis. DHS 132.45(4)(f)(2). Retention of records
- Office for Civil Rights “Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals”, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
- NIST Guidelines for Media Sanitization, Special Publication 800-88, December 2014, revision 1
- CMS Information Security ARS, Appendix A, CMSR High Impact Level Data, 9/20/13: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/downloads/ARS_App_A_CMSR_HIGH.pdf

** NEW POLICY **

INCIDENTS POLICY

Privacy & Security Incident Response, Breach Notifications, and Corrective or Disciplinary Actions

Purpose

The purpose of this policy is to establish consistent guidelines to effectively identify and handle Privacy Incidents, Security Incidents, corrective or disciplinary actions, and Breach of Unsecured PHI notifications. An incident response process is implemented to:

- Consistently detect, report, respond to and investigate incidents;
- Establish expectations for coordinating incident response across Chippewa County (herein County)
- Minimize loss, destruction, and impact;
- Mitigate the weaknesses that were exploited;
- Restore information system functionality and business continuity as soon as possible;
- Establish incident response communication requirements;
- Identify metrics to measure incident response capability and its effectiveness;
- Provide Breach of Unsecured PHI notifications as required;
- Establish a structured incident documentation process.

Responsible for Implementation

The Privacy Officer and Security Officer are responsible for implementing and overseeing this policy and procedure.

Policy

It is the policy of the County to:

1. Safeguard the confidentiality, integrity, and availability of Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other restricted as well as sensitive information, collectively "Confidential Information", through an established incident response process.

2. Consistently detect, report, respond to, contain, and correct privacy and security issues.

3. Minimize loss and destruction as well as mitigate other harmful effects, including for a known use or disclosure of PHI in violation of the County's policies and procedures or the HIPAA Privacy and Security Rules; restore information system functionality and business continuity as soon as possible; and make reasonable efforts to try to prevent incidents from reoccurring.

4. Quickly identify a Breach of Unsecured PHI and provide required notifications within the timeframe required by law.

5. Provide consistent corrective or disciplinary action for non-compliance with the Privacy and Security Rules and the County's privacy and security policies and procedures.

Incident Response Procedure

1. Identification Phase

a. Detection and Reporting

1. Clients, consumers, subscribers and other individuals may report complaints concerning the County's relevant privacy, security, and breach notification policies and procedures or its compliance with such policies and procedures to the Privacy Officer and/or Security Officer.

2. Workforce and other system users are required to report non-compliance with the County's privacy and security policies and procedures in accordance with the Information Privacy and Security Policy.

b. Upon receipt of a privacy or security incident report, the Privacy Officer and/or Security Officer or designee facilitates the following procedures:

1. Notifies and/or involves the County Administrator. Also notifies or involves the Department Head when appropriate and as needed for non-routine and significant incident investigations.

2. If the issue involved a known or suspected Breach of Unsecured PHI, Breach of client, consumer, and/or subscriber confidentiality, also refer to and follow the Breach of Unsecured PHI procedures below.

3. For privacy related reports:

a). If a Workforce member or Business Associate believes in good faith that the County engaged in unlawful conduct or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the organization endangers one or more client, consumer, subscriber, worker, or the public, he or she may disclose relevant PHI to:

1). A Health Oversight Agency or Public Health Authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the County or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the County; or

2). An attorney retained by or on behalf of the Workforce member or Business Associate for the purpose of determining the legal options of the Workforce member or Business Associate with regard to the conduct described in 1.b.3.a.

b). If a workforce member is a victim of a criminal act, he or she may disclose relevant PHI to a law enforcement official, provided that:

1). The PHI disclosed is about the suspected perpetrator of the criminal act; and

2). The minimum necessary PHI disclosed is limited to:

a. Name and address;

b. Date and place of birth;

c. Social security number;

d. ABO blood type and Rh factor;

e. Type of injury;

f. Date and time of treatment;

g. Date and time of death, if applicable; and/or

h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

4. For privacy and security related reports:

a). Completion of the Incident Identification and Incident Summary sections of the Privacy and Security Incident Report form (SIR form) in a clear and easy to understand way.

b). Facilitate providing a response to clients, consumers, subscribers, and other individuals (as appropriate) that report complaints without unreasonable delay and in no case later than 30 calendar days after receiving the complaint.

c). If the issue involves missing information, a Workstation, or Electronic Media, request the original be returned or destroyed and obtain verification of such and that it has not been copied, or accessed (as appropriate).

d). Collaborate with the County Administrator to determine whether to inform the County's insurance carrier of the issue (e.g. cyber and / or business insurance).

e). If the issue was a Privacy Incident, Precursor, or Indicator:

1). Resolve the issue and continue to monitor it as needed.

2). Complete the Follow-Up sections of the SIR form as appropriate.

f). If the issue was or is potentially a Security Incident:

1). Keeps the County Administrator apprised of the issue and progress to resolve. Also keeps the Department Head apprised when appropriate and as needed.

2). For non-technical Security Incidents, complete the investigation, implement preventative measures, resolve the Security Incident, and move to the Follow-up Phase below.

3). For technical Security Incidents, move to the Containment Phase below.

2. Containment Phase (Technical): Contain the Security Incident

a. The Security Officer, IT Director, or designee, in collaboration with appropriate Department Heads and appropriate contracted support vendors, facilitates the following, and/or works with vendors to address these items, as applicable:

1. Verifies that a qualified technical security resource is available to assist with efforts.

2. Evaluates the need to use forensic analysis, in consultation with Corporation Counsel.

3. Secures the physical and network perimeter.

a). If a decision is made to remove the system from the network for eradication, containment, and/or investigative purposes, consult with Department Heads.

b). Before the decision to freeze the system is made:

1). Remove volatile data from the system while it is still in its compromised state whenever possible.

2). Physically secure the physical area where the incident occurred.

3). Care should be taken not to alert the intruder to the actions.

c). Remove the network cable from affected system. *Do not reboot or make any changes to the system itself*.

4. Loads a trusted shell.

5. Retrieves any volatile data from the affected system.

6. Secures affected user accounts to prevent further unauthorized access.

7. Determines the relative integrity and the appropriateness of backing up the system.

   a). If appropriate, backs up the system.

   b). If appropriate, backs up the system using new media wiped with commercial software.

   c). Before forensics work is done on the backup, make a minimum of two extra binary copies of the backup itself.

      1). The original copy will be used for evidence, and properly stored and handled.

      2). A second backup will be used in forensic analysis by IT Security Representatives.

      3.) The third backup will be available for law enforcement.

   d). Protect backups and log them (refer to the Data Management policy)

8. Changes the password(s) to the affected system(s).

9. Determines whether it is safe to continue operations with the affected system(s).

   a). If it is safe, allows the system to continue to function.

      1). Complete documentation as described below.

      2). Move to the Follow-up Phase.

   b). If it is not safe to allow the system to continue operations, discontinue system(s) operation and move to Eradication Phase.

10. Analyzes the data and determine whether or not to initiate an Alert to organization users.

11. Issue alerts as deemed necessary.

b. The Security Officer and/or IT Director or designee keeps the County Administrator and Department Heads as appropriate, apprised of progress and documents:

1. All measures taken and communications made, including who completed activities and the start and end times of all efforts on the SIR form in a clear and easy to understand way.

2. As applicable and appropriate to the issue, create an evidence tag for each piece of evidence as outlined on the Chain of Custody Evidence Tag / Tracking Form. This provides evidence gathered during the Security Incident that can be used during prosecution.

c. Continue to the Eradication Phase.

3. Eradication Phase (Technical): Remove the cause, and the resulting security exposures, that are now on the affected system(s).

a. The Security Officer, IT Director, or designee, in collaboration with appropriate Department Heads and appropriate contracted support vendors, facilitates the following, and/or works with vendors to address these items, as applicable:

1. Determines symptoms and cause related to the affected system(s).

2. Strengthens the defenses surrounding the affected system(s), where possible (a risk assessment may be needed). This may include the following:

a). An increase in network perimeter defenses.

b). An increase in system monitoring defenses.

c). Remediate ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques, firewall/router changes, vulnerability patches applied, physical access control changes, etc.

3. Conducts a detailed vulnerability assessment to verify all the holes or gaps that can be exploited have been addressed. If additional issues or symptoms are identified, takes appropriate preventative measures to eliminate or minimize potential future compromises.

4. Contacts law enforcement.

b. The Security Officer and/or IT Director or designee keeps the County Administrator and Department Heads as appropriate, of progress and documents all measures taken and communications made, including who completed activities and the start and end times of all efforts on the SIR form in a clear and easy to understand way.

c. Continue to the Recovery Phase.

4. Recovery Phase (Technical): Restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

a. The Security Officer, IT Director, or designee, in collaboration with appropriate Department Heads and appropriate contracted support vendors determines if the affected system(s) has been changed in any way, and/or works with vendors to address these items, and as applicable:

1. Restores the system(s) to its proper, intended functioning.

a). Once restored, validates that the system functions the way it is intended or functioned in the past. This may require the involvement of the department and/or vendor that owns the affected system(s).

b). If operation of the system(s) had been interrupted (i.e., the system(s) was taken offline or dropped from the network while triaged), restarts the restored and validated system(s) and monitors for proper behavior.

2. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restarts the system and monitors for proper behavior.

3. Ensures the system is using latest configuration standards.

4. Performs a vulnerability assessment and penetration test using company-approved software and method as described in the System Build / Change Control Policy.

5. Updates system monitoring if necessary to alert to the specific vulnerability or attack in the future.

b. The Security Officer and/or IT Director or designee keeps the County Administrator and Department Heads as appropriate, apprised of progress and documents all measures taken and communications made, including who completed activities and the start and end times of all efforts on the SIR form in a clear and easy to understand way.

c. Client notifications. The Security Officer or designee:

1. Notifies affected organizations when there is a successful unauthorized access, use, disclosure, modification, or destruction of Confidential Information or interference with Confidential Information system operations in an information system.

2. Notifies other customers and/or clients of incidents that resulted in the misuse or potential or known inappropriate access of Confidential Information (e.g. unauthorized access, cyber intruder broke into an information system, lost or stolen unencrypted devices, inappropriate disposal, etc.).

3. Notifications include a general description of the incident and a County contact name, telephone number, email address and mailing address.

4. Also refer to the Breach of Unsecured PHI Procedures below for additional notification requirements.

d. Continue to the Follow-up Phase.

5. Follow-up Phase (Technical and Non-Technical): Review the Privacy Incident or Security Incident Form to look for "lessons learned" and determine whether the incident handling procedures could have been done in a better way.

a. It is recommended all incidents be reviewed shortly after resolution to determine where response could be improved for future issues.

b. The Privacy Officer, Security Officer, or designees shall review the incident documentation and complete the following (as applicable and appropriate):

1. Evaluate the cost and impact of the incident to the organization.

2. Determine what could be improved to prevent a similar incident of occurring in the future (e.g. update policies or procedures, provide additional training or reminders, purchase new technologies, etc.).

3. Complete the Follow-up / Lessons Learned section of the SIR form or create a "lessons learned" document and attach it to the SIR form.

4. Communicate findings to the County Administrator and Department Heads as appropriate.

5. Request approval for any implementation recommendations from the County Administrator as appropriate.

6. Carry out recommendations.

c. Close the incident.

Breach of Unsecured PHI Procedures

1. Discovery of Breach: A Breach of Unsecured PHI is treated as "discovered" as of the first day on which an incident that may have resulted in a Breach is known to the County.

a. County shall be deemed to have knowledge of an incident that may have resulted in a Breach if the incident is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or Agent (e.g. a Business Associate acting as an Agent of the County).

b. If a Business Associate (BA) is not an Agent of the County, then the knowledge of the incident is based on the day and time the BA notifies the County of the Breach.

2. Business Associate (BA) Responsibilities

a. A BA of the County that Accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, uses, or Discloses Unsecured PHI shall notify County of the Breach [1] without unreasonable delay and in no case later than one week after discovery of a Breach.

b. The notice shall include:

1. The identification of each individual whose Unsecured PHI was, or is reasonably believed by the BA to have been acquired, Accessed, used, or Disclosed in an unauthorized manner.

2. Any other available information that the County is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available (refer below).

c. The County, not the BA, will make the notifications described below, unless otherwise agreed upon by the BA and County (note: it is the burden of the County to document this notification).

d. Refer to the Business Associate policy for additional measures to resolve the issue.

3. Breach of Unsecured PHI Investigation: Following the discovery of a potential Breach, the Privacy and/or Security Officer shall begin an investigation (also refer to the Incident Response procedures) and facilitate the completion of the following, while documenting all measures taken:

a. Conducts a Breach of Unsecured PHI incident risk assessment to determine if an impermissible use or Disclosure of PHI constitutes a Breach of unsecured PHI and whether it requires notifications be made to individuals, media, or the HHS secretary.[2] If an incident risk assessment is not completed, the County assumes a Breach of Unsecured PHI occurred and makes recommendations that notifications are made, as outlined below.

1. An "acquisition, Access, use, or Disclosure in a manner not permitted is presumed to be a breach unless, as applicable, it is demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment" of at least the following factors:

a). The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

b). The unauthorized person who used the protected health information or to the Disclosure was made;

[1] The organization may choose to make the decision to notify clients, consumers, and subscribers of a Breach even after completion of the risk assessment indicates that there is no requirement to do so.
[2] The organization may choose to make the decision to notify clients, consumers, and subscribers of a Breach even after completion of the risk assessment indicates that there is no requirement to do so.

c). Whether the protected health information was actually acquired or viewed; and

d). The extent to which the risk to the protected health information has been mitigated.

2. Utilize the "Breach Risk Assessment Tool" to complete this assessment. Also refer to the "Privacy and Security Violations Breach Notification Recommendations" Form which includes types of violations and Breach of Unsecured PHI notification recommendations.

3. The incident risk assessment is documented as part of the investigation in the SIR form noting the outcome of the incident risk assessment process.

4. Notifications:

a. Timeliness.

1. Upon determination that a Breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the incident that resulted in a Breach by the County or BA involved that is acting as the County's Agent.

2. Delay of Notification is Authorized for Law Enforcement Purposes. When a Law Enforcement Official informs the County that a notification, notice, or posting would impede a criminal investigation or cause damage to national security:

a). If this statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or

b). If this statement is made orally, document the statement, including the identity of the Law Enforcement Official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

b. Content of the Notice:

1. The notice shall be written in plain language and contain the following information:

a). A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

b). A description of the types of Unsecured PHI involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

c). Any steps the individual should take to protect themselves from potential harm resulting from the Breach.

d). A brief description of what action(s) the County is taking to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches.

e). Any procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

2. County will assess the facts and circumstances of breaches of unsecured PHI on a case by case basis and determine at that time whether there is any need for translation or an alternative format of this notification[3]

c. Methods of Notification: The method of notification used is based on the individuals or entities notified, as follows:

1. Notifications to Individual(s)

a). Written notification by first-class mail to the individual at his or her last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by secure electronic mail.

1). The notification may be provided in one or more mailings as more information becomes available.

2). If the County knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative.

3). In the limited circumstance that an individual affirmatively chooses not to receive communications from a health care provider at any written addresses or email addresses *and* has agreed only to receive communications orally or by telephone, the provider may telephone the individual to request and have the individual pick up their written breach notice from the provider directly. In cases in which the individual does not agree or wish to travel to the provider to pick up the written breach notice, the health care provider should provide all of the information in the breach notice over the phone to the individual, document that it has done so, and the Department will exercise enforcement discretion in such cases with respect to the ‘‘written notice’’ requirement.

[3] Organizations that receive Medicaid, CHIP or Medicare Part C payments may have obligations under Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act of 1990 laws to provide breach notifications to individuals in alternative languages, and in alternative formats, such as Braille, large print, or audio)

b). Substitute Notice: When there is insufficient or out-of-date contact information (including an address, phone number, email address, etc.) that prevents direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual is provided. A substitute notice does not need to be provided when there is insufficient or out-of-date contact information that prevents written notification to the individual and next of kin or personal representative.

1). When there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

2). When there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice is in the form of either a conspicuous posting for a period of 90 days on the County's website home page, or a conspicuous notice in a major print or broadcast media in the County's geographic areas where the individuals affected by the Breach likely reside. Include a toll-free number in the notice that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the Breach. This substitute notice must be provided as soon as reasonably possible and in no case later than 60 calendar days from discovery of the breach.

c). If the notification requires urgency because of possible imminent misuse of Unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

2. Notifications to the Media

a). The Notice is provided in the form of a press release to the media by the individual stated in the above Working with the Media procedures, utilizing the Sample Notification Letter to the Media.

1). What constitutes a prominent media outlet differs depending upon the State or jurisdiction where the County's affected clients, consumers, and/or subscribers reside. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily

circulation throughout the city, even though the newspaper does not serve the whole State.

b). Notifications are provided to prominent media outlets serving the state and regional area (of the breached clients, consumers, subscribers) when the Breach of Unsecured PHI affects more than 500 of the County clients, consumers, subscribers.

c). Client, consumer, subscriber identifiers are not included in these notifications as they are publicly available.

3. Notifications to the Secretary of HHS

a). Client, consumer, and subscriber identifiers are not included in these notifications as the information may be made publicly available.

b). For Breaches involving 500 or more individuals, the County notifies the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

c). For Breaches involving less than 500 individuals:

1). Submit the notification when sending notifications to individual.

2). Notifications are made here: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

4. Notifications to Other Organizations:

a). The County is not a business associate of any other organization, and therefore, does not have nor need any procedures to provide notifications to other organizations.

5. Notification Inquiries. Refer to the Talking Points to Respond to Breach of Unsecured PHI Inquiries Form for examples of how to respond to inquiries on Breaches. Tailor responses based on the type and severity of the Breach.

Investigation and Sanction Procedures

Refer to the Information Privacy and Security Policy for Investigation and Sanctions procedures.

Training

1. New Workforce members receive privacy and security training within their first month, but no later than three months, of employment.

2. Existing Workforce members and system users shall be trained annually.

3. Training content shall include:

   a. Privacy and security policies and procedures with respect to PHI and ePHI and other Confidential Information as necessary and appropriate to carry out their job responsibilities and prevent security violations and incidents from happening.

   b. How to identify and promptly report known and suspected Privacy Incidents, security violations and incidents, and Breaches within the County, as well as return or destroy PHI, as appropriate for the incident.

   c. How to assist in investigating, documenting, and resolving incidents and breaches of Unsecured PHI for Workforce who will need to complete these activities

Documentation

1. The Privacy Officer, Security Officer and/or designee maintains all of the following documentation in a secure location for a period of seven (7) years after the conclusion of the investigation:

   a. All documentation of complaints and investigations including all incident response forms, notes, meeting minutes, corrective or disciplinary actions provided, actions taken to prevent future occurrences, and other items relevant to the investigation.

   b. All documentation related to Breach of Unsecured PHI investigations, including the risk assessment and notifications made.

   c. Note: the County has the burden of proof for demonstrating that all notifications were made or that an Access, acquisition, use or Disclosure did not constitute a Breach, as well as evidence demonstrating the necessity of a delay authorized by Law Enforcement (when applicable).

Filing a client, consumer, subscriber privacy or security–related complaint to the Office for Civil Rights (OCR)

1. Clients, consumers, and subscribers may file complaints to the OCR by:

   a. Mailing the complaint to:

      Centralized Case Management Operations
      U.S. Department of Health and Human Services
      200 Independence Avenue, S.W.
      Room 509F HHH Bldg.
      Washington, D.C. 20201

   b. Using the online Complaint Portal available at http://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html

2. During such investigation, the Security Officer and/or Privacy Officer shall assist the CMS Administrator to resolve the complaint.

Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Resources

- HIPAA COW Security Incident Response Policy, Version 8, 7/11/05
- HIPAA COW Breach Notification – Protected Health Information for Covered Entities Policy, Version 6, 3/5/13
- HIPAA COW Security Oversight Policy/Procedure, Version 2, 4/19/05
- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide, August 2012
- SANS Sample Incident Handling Forms
- Incident Contact List
- Incident Identification
- Incident Survey
- Incident Containment
- Incident Eradication
- Incident Communication Log

Applicable Standards/Regulations

- HIPAA Final Omnibus Rule, January 25, 2013
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules
- 45 CFR § 164.308(a)(1)(i) HIPAA Security Rule Security Management Process
- 45 CFR § 164.308(a)(6)(i) HIPAA Security Rule Security Incident Procedures
- 45 CFR § 164.308(a)(6)(i)(ii) HIPAA Security Rule Response and Reporting
- 45 CFR § 164.308(a)(1)(ii)(C) HIPAA Security Rule – Sanction Policy
- 45 CFR – Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information
- 45 CFR § 164.512(f)(2)(i) HIPAA Privacy Rule Permitted disclosures: Limited information for identification and location purposes
- 45 CFR § 164.502(j) Disclosures by whistleblowers and workforce member crime victims
- 45 CFR § 164.502(j)(1) HIPAA Privacy Rule Disclosures by whistleblowers
- 45 CFR § 164.502(j)(2) HIPAA Privacy Rule Disclosures by workforce members who are victims of a crime
- 45 CFR § 164.530(d)(1) HIPAA Privacy Rule Complaints to the Covered Entity
- 45 CFR § 164.530(d)(2) HIPAA Privacy Rule Documentation of complaints
- 45 CFR § 164.530(e)(1-2) HIPAA Privacy Rule Sanctions and Documentation
- 45 CFR § 164.530(f) HIPAA Privacy Rule Mitigation

** NEW POLICY **
INFORMATION SECURITY RISK MANAGEMENT POLICY

Purpose

The purpose of this policy is to establish the organization's information security risk management program intended to support and protect Chippewa County and its ability to fulfill its mission and effectively and consistently protect its information assets. Risk management is the process of identifying, assessing, and taking steps to reduce risk to an acceptable level. Not understanding the risks introduced with changes or implementation of new controls, assets and procedures could expose Electronic Protected Health Information and other restricted as well as sensitive information, collectively "Confidential Information" to hostile parties.

Completing a risk analysis and ongoing monitoring are mechanisms to help Chippewa County identify potential threats and vulnerabilities to the confidentiality, integrity, and availability of Confidential Information the organization creates, receives, maintains, and transmits. Risk analysis and ongoing monitoring also provides a formalized process to understand current information security controls, leading practices to safeguard Confidential Information, and known threat sources.

This information is then utilized to make risk-based, prioritized recommendations for improvement. Efforts are then applied to eliminate or reduce vulnerabilities and threat capabilities to reasonable and appropriate levels. Ultimately, the information security risk management program is a critical function designed to improve the security posture and maturity of the organization. It establishes a framework to manage risks and creates boundaries to informed make risk-based decisions. The risk management process included in this policy and procedures are based on key steps outlined the National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (NIST SP 800-30), version 2002.

The steps should be customized to most effectively identify risk for the organization based on its own uniqueness. Even though these items are listed as steps, they are not prescriptive in the order that they should be conducted. Some steps can be conducted simultaneously rather than sequentially.

Goals

To develop a framework throughout the organization to:

1. Continuously assess risk to the confidentiality, integrity, and availability of Confidential Information
2. Identify and document current administrative, physical, and technical controls
3. Identify potential and known information security risks
4. Prioritize identified risks
5. Develop and implement reasonable and appropriate plans to address information security risks
6. Ensure practices are appropriately modified to address changes occurring in the business and in the external threat environment
7. Document efforts to eliminate or reduce information security risks

8. Enable management to make well-informed information security risk management decisions to justify the expenditures that are part of the information security budget

Responsible for Implementation

The following are responsible for implementing and overseeing this policy: Privacy Officer, Security Officer, IT Division and Risk Management Team members.

The Risk Management Team is responsible for:

1. Authorizing and overseeing the process of completing risk analyses
2. Approving mitigation plans
3. Ensuring risk mitigation controls are applied

Risk Management Team members include:

1. Security Officer
2. Privacy Officer
3. Information Technology Director
4. Human Services Fiscal Manager
5. Public Health Fiscal Manager

Policy

1. It is the policy of Chippewa County to:

    a. Conduct risk assessments of the potential Threats and Vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information (ePHI) and other restricted as well as sensitive information, collectively "Confidential Information"; and

    b. Develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's information security program.

2. Risk analysis and risk management are recognized as important parts of the organization's security compliance program. At a minimum, they are completed in accordance with the Risk Analysis and Risk Management requirements in the HIPAA Security Rule.

    a. To the extent possible, risk assessments are done throughout system life cycles:

        1. Before the purchase or integration of new technologies and prior to changes made to physical safeguards;

        2. While integrating technology and making physical security changes, and

        3. Into sustainment and monitoring of appropriate security controls.

b. Information system technologies are not deployed unless the technology is widely-used, as well as generally accepted as stable, reliable, and fit for its intended purpose. Exceptions are made only if purchase commitments are preceded by both a risk assessment and the approval of the Security Officer.

c. The organization performs periodic technical and non-technical assessments of the security rule requirements in response to environmental or operational changes affecting the security of Confidential Information.

3. Risk is managed through the implementation of security controls which are dictated based on the level of sensitivity and/or value the information assets provide to the business as well as the level of risk to which those assets are subject (refer to the Information Classification Table). To the extent possible, Chippewa County implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

a. Ensure the confidentiality, integrity, and availability of all Confidential Information the organization creates, receives, maintains, and/or transmits;

b. Protect against any reasonably anticipated Threats or hazards to the security or integrity of this information;

c. Protect against any reasonably anticipated uses or disclosures of Confidential Information that are not permitted or required; and

d. Ensure compliance by workforce.

e. All workforce members are expected to fully cooperate with all persons charged with doing risk management work.

Procedures

1. Risk Assessment

The intent of completing a risk assessment is to determine potential Threats and Vulnerabilities and the likelihood and impact should they occur. The following steps are utilized to conduct a full risk assessment, unless a contractor/consulting organization is hired that utilizes a different and acceptable risk assessment approach. Some of the steps are also utilized by the Risk Management Team or others as delegated when purchasing, upgrading, or moving Confidential Information systems and other applications or technologies and as needed to assist in the organizations risk management efforts; also refer to the System Build / Change Control Policy. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

a. <u>Step 1. System Characterization</u>

1. Identify where Confidential Information is created, received, maintained, processed, or transmitted. Consider policies, laws, remote workforce and

telecommuters, removable media and portable computing devices (e.g., computers, laptops, removable media, and backup media).

2. When changing, purchasing or otherwise introducing new applications or technologies into the production environment:

   a). Refer to the System Build / Change Control policy and procedures.

   b). Document the classification of the highest data criticality / data sensitivity level (refer to the Information Classification Table and Information Classification Questionnaire)

b. Step 2. Threat Identification

Identify and document potential Threats (the potential for Threat Sources to successfully exercise a particular Vulnerability).

c. Step 3. Vulnerability Identification

1. Develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential Threat Sources.

2. This step may include testing systems, penetration testing, etc. Vulnerability Assessments are completed as described in the System Build / Change Control policy, procedures, and standards.

d. Step 4. Control Analysis

Document technical and non-technical controls (policies, procedures, physical security measures) (e.g. complete a physical walkthrough on Chippewa County's data processing areas, locations containing infrastructure systems, workstations, and other areas that contain Confidential Information), training, technical mechanisms and functionalities, insurance, etc.) that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a Threat Source exploiting a Vulnerability and reduce the impact of such an adverse event.

e. Step 5. Likelihood Determination

1. Determine the overall likelihood rating that indicates the probability that a Vulnerability could be exploited by a Threat Source given the existing or planned security controls.

2. Utilize a scoring mechanism, such as the one in NIST Special Publication (SP) 800-30; low (.1), medium (.5), or high (1).

f. Step 6. Impact Analysis

1. Determine the level of adverse impact that would result from a Threat Source successfully exploiting a Vulnerability.

2. Factors to consider should include the importance to the organization's mission; sensitivity and criticality of the Confidential Information (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.

3. Utilize a magnitude of impact rating, such as the one in NIST SP 800-30; low (10), medium (50), or high (100).

g. Step 7. Risk Determination

1. Calculate a risk level.

2. One approach that may be utilized is to multiply the NIST SP 800-30 likelihood rating by the impact rating; Risk level of low (1-10), medium (>10-50) or high (>50-100).

3. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given Vulnerability were exercised.

h. Step 8. Control Recommendations

1. Identify controls that could reduce or eliminate the identified risks to an acceptable level, as appropriate to the organization's operations. Factors to consider may include level of sensitivity and/or value the information assets, level of risk to which assets are subject, effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability.

2. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

i. Step 9. Results Documentation

1. Document results of the risk assessment, such as in a Risk Summary and/or Risk Mitigation Implementation Plan.

2. Provide a summary of the results to the County Administrator.

2. Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of Confidential Information. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the Organization consistent with its goals and

mission. The following steps may be utilized to make determinations of the appropriate controls to put into place. Some of the steps may also be utilized when purchasing, upgrading, or moving Confidential Information systems and other applications or technologies and as needed to assist in the organizations risk management efforts.

a. Step 1. Prioritize Actions

b. Step 2. Evaluate Recommended Control Options

Using results from Step 7 of the Risk Assessment and after obtaining approvals in Step 9, identify and sort top risks (Vulnerability-Threat pairs), such as from high to low.

Review the recommended control(s) from Step 8 as well as alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. Select a "most appropriate" control option for each Vulnerability-Threat pair, and document reasons for not selecting other controls.

Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction), of applying a control with its subsequent cost of application.

c. Step 3. Conduct Cost-Benefit Analysis

d. Step 4. Select Control(s)

Taking into account the information and results from previous steps, the organization's mission, and other important criteria, determine the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of Confidential Information. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

e. Step 5. Assign Responsibility

Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources (e.g. time, money, etc.) needed for the successful implementation of controls.

f. Step 6. Develop Safeguard Implementation Plan

1. Develop an overall implementation or action plan. Include the following information, as applicable:

a). Each risk or Vulnerability/Threat pair and risk level
b). Prioritized actions
c). The recommended feasible control(s) for each identified risk
d). Required resources for implementation of selected controls
e). Team member responsible for implementation of each control

f). Start date for implementation
g). Target date for completion of implementation
h). Maintenance requirements

2. Obtain written approval for decisions on policy, procedure, budget, system operational and management changes, as well as acceptance of remaining risk for systems that create, receive, maintain, transmit or otherwise impact from the Department of Administration or the County Board of Supervisors.

g. Step 7. Implement Selected Controls

As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.

1. Document the date controls are put into place.

2. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

3. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

4. Provide regular status reports to the County Administrator and other key stakeholders, as appropriate.

h. Any remaining (residual) risk after other risk controls have been applied requires sign off by the County Administrator.

3. Risk Management Schedule

The two principle components of the risk management process (Risk Assessment and Risk Mitigation) are carried out according to the following schedule to ensure the continued adequacy and continuous improvement of the organization's information security program.

a. Risk Assessment

1. Scheduled Basis – Conduct an overall risk assessment of the organization's information system infrastructure and policies and procedures in place to safeguard the confidentiality, integrity and availability of Confidential Information at least every two (2) years when possible, but at a minimum every four (4) years.

2. Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed, ongoing assessments of the potential security Threats and Vulnerabilities to a system are

done (e.g. when purchasing, upgrading, changing, or moving Confidential Information systems). Refer to the System Build / Change Control policy.

3. As Needed –a full or partial risk assessment in response to environmental or operational changes affecting the security of Confidential Information may be done (e.g. when experience a security incident, turnover in key workforce members/management, other things that impact how Confidential Information is stored or transmitted, or there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information).

4. Ongoing Monitoring – Ongoing monitoring ensures that the risk reduction process is continuous instead of a one-time or annual event. Risk mitigation activities and trends are monitored on a regular, ongoing basis.

b. Risk Mitigation – to the extent possible, selected security controls are put in place as described in the risk mitigation implementation plan or other plan developed during the risk assessment process.

4. Insurance

Chippewa County has business, privacy breach response management, information security, and cyber security insurance to cover potential claims.

5. Documentation

Maintain documentation of all risk assessment and risk mitigation efforts, including decisions made on what controls to put in place as well as those to not put into place, for a minimum of six years.

6. Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms, refer to the HIPAA Privacy and Security Definitions form located on the Employee Portal under Policies.

Resources

- NIST Risk Management Guide for Information Technology Systems, SP 800-30, July 2002.
- NIST Security Self-Assessment Guide for Information Technology Systems, SP 800-26, August 2005
- NIST Managing Information Security Risk SP 800-39, March 2011
- NIST Guide for Mapping Types of Information and Information Systems to Security Categories, SP 800-60, August 2008
- Draft HIPAA COW Risk Management Policy, November 2012

Applicable Standards/Regulations

- 45 CFR § 164.308(a)(1)(i) HIPAA Security Rule Security Management Process
- 45 CFR § 164.308(a)(1)(ii)(A) HIPAA Security Rule Risk Analysis
- 45 CFR § 164.308(a)(1)(ii)(B) HIPAA Security Rule Risk Management
- 45 CFR § 164.308(a)(8) HIPAA Security Rule Evaluation

** NEW POLICY **

FACILITY ACCESS AND PHYSICAL SECURITY POLICY

Purpose

Controlling physical access into buildings, areas within them, and when transporting information provides mechanisms to safeguard Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other Restricted Information as well as Sensitive Information from unauthorized access, use, disclosure, and modification. This also protects the safety of Workforce and visitors. The purpose of this policy and related procedures is to establish minimum facility access and physical safeguards to control access to this information within Chippewa County's (herein County) facilities, as well as when it is taken offsite. It is the goal of the organization to effectively protect physical assets and human resources.

Responsible for Implementation

The Privacy Officer, Security Officer, Information Technology Director, Human Resources Division, and Facilities and Parks Division are responsible for implementing and overseeing this policy and procedure.

Policy

It is the policy of the County to:

1. Safeguard the facility and Confidential Information from unauthorized physical access, tampering, and theft.

2. Limit physical access to hardcopy, Workstations, and information systems that create, receive, maintain, and/or transmit, Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other restricted as well as sensitive information, collectively "Confidential Information", as well as the facilities where they are housed to only those that need access.

3. Control and validate access to facilities.

4. Provide a safe environment for Workforce and visitors.

5. Safeguard Confidential Information when taken off the premises.

Procedures

1. <u>Identification of Individuals in the Organization</u>

    a. Refer to the Identification and Access Card policy for requirements for issuing and wearing ID cards and Electronic Access Devices.

2. Individuals Allowed in Restricted Areas

a. Workforce members as approved by their supervisor and as needed to perform their job duties.

b. Consumers, clients, and subscribers and their family/friends with an escort of a Workforce member into and out of the Restricted Areas.

c. Workforce members' family members and friends visiting (briefly) with the escort of a Workforce member.

d. Vendors with a Workforce member's escort into and out of the areas for brief periods of time as long as:

1. To the extent feasible, Confidential Information is not visible or being discussed;

2. A Business Associate Agreement is in place with the vendor; or

3. The individual signed a confidentiality agreement.

e. Vendors approved by a Department Head or their designee, once acclimated to the areas, without an escort. Applicable agreements must be in place as described in the Business Associate and Service Provider policies.

f. Individuals who do not have access to Restricted Areas may not attempt to circumvent security or forcibly attempt to enter Restricted Areas.

3. Individuals Allowed in Unrestricted Areas

All Workforce members, consumers, clients, subscribers, Vendors, contractors, and other visitors may be in Unrestricted Areas. Note: if they need to go through a Restricted Area to access an Unrestricted Area, they are escorted by an authorized Workforce member to the Unrestricted Area, unless otherwise allowed.

4. Facility Security Controls (Doors)

a. Access to the County's exterior and interior room doors are locked with one or more of the following, depending on the facility location:

1. Keyed locks.

2. Cypher code locks.

3. Software based access control system – electronic access device.

b. Keys (and other lock entry mechanisms).

1. The least number of keys and other lock entry mechanisms shall be distributed.

   a). Distribution is limited so that only the minimum necessary number of individuals is able to access the facilities and specified locked interior rooms.

   b). Distribution decisions are based on the organization's needs. This includes the ability for key individuals to access Confidential Information systems during emergencies.

2. The Facilities and Parks Division secures all unused keys in locked cabinets inside a locked office (excluding the Sheriff's Department, Jail, Highway Department, and forest management gates)

   a). Refer to the Key Issuance and Request Policy for distribution, collection, and additional safeguarding of keys requirements.

3. Cypher codes

   a). Department Head or designee maintains a list of individuals with cypher codes, their assigned roles, issuance dates, change dates and termination dates.

   b). When an individual's role changes, the Department Head or designee immediately (or as soon as practicable) ensures that cypher codes continue to be appropriate for his or her role.

   c). Cypher code lock combinations are changed:

      1). Every four years; and

      2). When an individual that knows the code no longer needs the code and there is deemed a high risk of an unauthorized attempt to enter the door.

c. Reasonable controls will be implemented in rooms or areas that store Confidential Information (e.g. the area is monitored at all times by an authorized individual) as appropriate to monitor and secure Confidential Information.

5. <u>Servers and Data Wiring Safeguards</u>

a. Physical access to servers, data wiring, data processing areas, and other related equipment shall be limited to those individuals able and authorized to maintain and/or restore access to them.

   1. Servers are in a locked room inside the IT Division with electronic access device access and key access to the door in the hallway. There are two cameras in the server room.

2. Access rights to the server room shall be provided on a strict "need to have" basis as determined by the IT Director, Security Officer and Facilities & Park Director.

3. Data wiring closets, or network devices, are in locked rooms with key access. There are cameras in the hallways that capture who enters / leaves these rooms.

4. Doors to server rooms:

   a). Shall be mounted with the hinges located on the inside of the room. If this is not possible, hinge pins are spot welded or "pinned" to prevent their removal.

   b). Shall not have vents. If vents are needed for airflow, they are mounted on the inside of the door and reinforced to prevent access.

   c). Shall not be self-closing.

5. Walls surrounding server rooms shall run from floor to ceiling or deck to prevent anyone from climbing over the wall to gain access through a false ceiling.

6. For doors that have an electronic access device, key access is only authorized to be used as a means of over-riding the electronic access device system in the event emergency access is required.

7. The Human Resources Division (electronic access) and Facilities and Parks Division (keys) maintains a list of individuals authorized to access these rooms.

8. Human Resources Division shall:

   a). Review the electronic access device list on an annual basis;

   b). Remove individuals from the list when access is no longer required or needed after discussing with the Department Head and/or County Administrator.

b. To help prevent tampering data or telecommunication cables located outside of areas controlled by the County are placed:

   1. Above drop ceilings;

   2. In a wiring management system; and/or

   3. Inside protective conduit.

c. IT Division, Server Room, and Data Wiring Access

1. The IT Division (for purposes of this section, the IT Division includes the server room) is a secured and Restricted Area

   a). Access shall be granted to only those individuals who have a mission-essential business need. Vendors and service personnel must have contracts and/or agreements in place as required by the Business Associate and Service Provider policies

   b.) IT Division contains data, which is Restricted and Sensitive, personal in nature, and in some cases, protected by law.

   c). IT Division is not a common workspace; therefore, traffic in the IT Division shall be kept to a minimum.

   d). Access to the server room, by anyone other than an employee that accesses using an electronic access device, requires signing in and out on a log outside the room(s).

      1). Record on Data Center Sign-in Sheet: date, visitor name, visitor's company name, individual or department visiting, reason for entry, in time, and out time.

      2). Sign-in sheets are reviewed and maintained by the IT Director on a monthly basis.

2. IT Division access falls under the following three categories:

   a). Unaccompanied 24 X 7 Access: This level of access shall be granted to the least possible number of Workforce (IT personnel and Facilities and Parks Division).

   b). Accompanied Access: Those with Accompanied Access shall be allowed access to the IT Division, only with those who are appropriately badged for Unaccompanied 24 X 7 Access. When an authorized Workforce member acts as the escort, that Workforce member, or by an IT Division Workforce member (if agreed upon in advance), shall remain in the IT Division during the visit. The escort assumes responsibility for the actions of those they allow into the IT Division and are responsible to ensure they have not removed items of equipment, media, or data.

   c). No Access: Everyone who is not otherwise cleared is in this category. There is no implied consent for access based on one's status as a County Workforce member, or a contractor of Chippewa County.

3. In general, any access, which is not specifically approved, is denied

4. Only Workforce members that are issued an electronic access device with access to the room have the authority to escort individuals into the room. Approvals for completing work in the room shall be obtained by the IT Director or designee.

5. The IT Director may request reports on a periodic basis to review the access.

6. Electronic access devices and keys are not transferable.

7. Actual or suspected loss of an electronic access device shall be reported immediately to the Human Resources Division. Deactivation shall occur at reporting time. At no time shall an electronic access device be left active while a search is taking place. IT Division electronic access devices generally also have access to exterior building doors, so it is critical to report suspected losses immediately.

8. IT Division and Server Room Emergency Access

   a). In the event of fire, natural disaster, chemical spill, or any other event, which would render the IT Division and/or Server Room uninhabitable, the IT Division will be evacuated immediately. The appropriate emergency personnel shall control access to the site during the entire course of the emergency.

   b). Once access is granted, the IT personnel will enter to make an initial assessment of the condition of the IT Division, server room, and equipment.

   c). If conditions render the site usable, systems shall be allowed to remain running, and IT personnel shall access the IT Division and server room to make an assessment and take appropriate remedial action.

   d). If the site can be accessed, but is not usable or suitable for continued use, IT personnel shall be called into the IT Division to begin a process of an orderly shutdown, and begin removing equipment, racks, etc. that are functional or may be repairable. Priority will be given to the safety of personnel, and to evacuating as much equipment as possible to a safe indoor location, or a safe and guarded outdoor location, until it can be moved to a better location. Precise procedures and instructions will depend on the nature and extent of the emergency. The IT personnel on site shall direct the effort, and work with other agencies to secure help to move and transport equipment.

   e). Movement, repair and restoring of service will be prioritized. Systems, tapes and networking devices shall be secured in accordance with the level of security of the information that remains.

f). If the building is structurally dangerous, the minimum personnel necessary may be allowed into the IT Division and server room to retrieve as much as can be safely removed.

6. Additional Facility Safeguards

a. Refer to the Information Privacy and Security and Facility Use policies for additional security requirements.

b. There are motion-detecting surveillance cameras throughout the Courthouse building. Two motion detection surveillance cameras are in the server room.

1. They stream continuously and record when motion is detected.

2. Recordings are maintained for 30 days, unless required for a specific investigation that requires an additional retention period.

3. Recordings are not routinely checked. They are usually only reviewed in the event there is a need to review them due to an incident, such as the investigation of theft, vandalism, or violation of policy, state, or federal law.

c. Refer to the Surveillance Camera policy for additional information regarding the surveillance cameras.

7. Documentation

All documentation related to this policy and procedure is maintained by the Security Officer, IT Division, Human Resources Division, and Facilities and Parks Division for six years from the date of creation or last date in effect, whichever is later.

a. Reporting and Compliance

Refer to the Privacy and Security Oversight policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Reporting and Compliance

Refer to the Information Privacy and Security policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Resources

- SANS Clean Desk Policy, June 2014
- HIPAA COW Facility Access Policy, Version 6, 4/4/05

Applicable Standards/Regulations

- HIPAA Final Omnibus Rule, January 25, 2013
- 45 CFR § 164.308(a)(7)(ii)(C) HIPAA Security Rule Emergency Mode Operation Plan
- 45 CFR §164.310(a) HIPAA Security Rule Facility Access Controls
- 45 CFR §164.310(a)(2)(ii) HIPAA Security Rule Facility Security Plan
- 45 CFR §164. 310(a)(2)(iii) HIPAA Security Rule Access Control and Validation Procedures
- Wis. HFS 92, Nov. 2008
- NIST Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, revision 4, April 2013

** NEW POLICY **

KEY ISSUANCE AND REQUEST POLICY

Purpose

Chippewa County Key Issuance and Request Policy shall be used to distribute and collect keys to ensure the safety and security of Chippewa County property and personnel based on the integrated security plan recommendation.

Responsible for Implementation

The Facilities and Parks Division and the Human Resources Division are responsible for implementing and overseeing this policy and procedure.

Policy

For the safety and security of the public, Chippewa County (herein County) Workforce members and facilities, it is the policy of the County to safeguard the facility and Confidential Information from unauthorized physical access, tampering, and theft through restricted distribution of keys.

This policy will affect the Chippewa County facilities and grounds excluding:

- Sheriff's Department
- Jail
- Highway Department
- Forest Management Gates
- Communication Towers
- All County Vehicles

Issuing New Keys to New Employees

1. Access requested and provided is limited so that only the minimum necessary number of individuals is able to access the facilities and specified locked interior rooms.

2. The Department Head shall complete a Request for Access Form (RFA) and submit it to Human Resources (HR) at least two (2) weeks prior to the new employee's start date. The Human Resources Division may approve an exception to the two (2) week requirement in rare situations.

3. The Human Resources Division shall notify the Facilities and Parks Division when a new employee is hired by emailing a copy of the RFA to the Facilities and Parks Administrative Assistant.

4. The Facilities and Parks Administrative Assistant will initiate the Key Request Form and email it to the applicable Department Head or designee for confirmation of request and signature authorization.

5. Upon confirmation and receipt of the Key Request Form, the Facilities and Parks Division will prepare key(s) for pickup within 7-10 business days.

6. The Facilities and Parks Administrative Assistant will send an email notification to the Department Head when the key(s) are ready for pickup in the Facilities and Parks Division office.

7. The Facilities and Parks Division shall maintain a list of individuals with keys and their assigned access roles. The list was initiated in September 2015 and includes individual's names assigned keys from that date forward.

8. **The employee is required to pick up and sign for keys in the Facilities and Parks Division office, no exceptions.**

9. When an employee's role changes, the Department Head immediately, or as soon as practicable, shall collaborates with Human Resources Division and the Facilities and Parks Division to ensure that keys continue to be appropriate for his or her role. This may include completing a new RFA.

10. Refer to the Facility Access Control policy for additional key and facility security requirements.

Returning Keys from Exiting Employees Leaving County Employment

1. Department Head or Supervisor shall notify the Human Resources Division when an employee is leaving County employment.

2. The Human Resources Division shall notify the Facilities and Parks Division when an employee is leaving County employment by sending an email to the Facilities and Parks Administrative Assistant.

3. The employee shall return the key to the Facilities and Parks Division on or before their last day of work. If this isn't possible to do so, the employee shall return it to the Human Resources Division or the Department Head. Then, the Human Resources Division or Department Head shall return the key to the Facilities and Parks Division.

4. The Facilities and Parks Administrative Assistant will log the return of key(s) from the employee on the original Key Request Form.

NOTE: Issuance of new keys may be delayed for new employees due to non-compliance with this policy. If keys are not returned, a service charge of $100 per key may be assessed to the department or to the employee for replacement and/or rekeying costs.

Internal Transfers

1. If a transfer is approved, the Department Head is responsible for completing the RFA form and Office Relocation Form and forwarding it to the Human Resources Division at least two (2) weeks prior to the employee's transfer date. The Human Resources Division may approve an exception to the two (2) week requirement in rare situations.

2. The Human Resources Division shall notify the Facilities and Parks Division when an employee has been approved to transfer or move internally in the County by emailing a copy of the RFA form.

3. The Facilities and Parks Administrative Assistant will initiate the Internal Key Request Form for Moves and email it to the applicable Department Head or designee for confirmation of request and signature authorization.

4. Upon confirmation and receipt of the Key Request Form the Facilities and Parks Division will prepare key(s) for pickup within 7-10 business days.

5. The Facilities and Parks Administrative Assistant, if applicable, will send an email notification to the Supervisor and Employee when the key(s) are ready for pickup in the Facilities and Parks Division office.

6. **The employee is required to return past issued key(s), pick up new key(s), and sign for key(s) in the Facilities and Parks Division office, no exceptions.**

NOTE: All unused keys will need to be returned to the Facilities and Parks Division prior to issuance of new key(s). The Human Resources Division will remind both the transferring employee and the Facilities and Parks Administrative Assistant that the keys no longer needed, associated with former position, will need to be returned when they pick up the new key(s) for the new position.

Reporting and Compliance

Refer to the Information Privacy and Security policy for requirements to reporting suspected and known non-compliance of this policy and procedure as well as potential outcomes for violations.

Key Definitions

For capitalized terms refer to the HIPAA Privacy and Security Definitions document.

Applicable Standards/Regulations

- HIPAA Final Omnibus Rule, January 25, 2013
- 45 CFR §164.310(a) HIPAA Security Rule Facility Access Controls
- 45 CFR §164.310(a)(2)(ii) HIPAA Security Rule Facility Security Plan
- 45 CFR §164. 310(a)(2)(iii) HIPAA Security Rule Access Control and Validation Procedures