CHIPPEWA COUNTY

EXECUTIVE COMMITTEE

REGULAR MEETING

SEPTEMBER 16, 2025

CHIPPEWA COUNTY COURTHOUSE, RM 302

4:00 PM

1. CALL TO ORDER

Chair Hull called the meeting to order at 4:00 p.m.

2. ROLL CALL

Attendee Name	Organization	Title	Status	Arrived
Chuck Hull	Chippewa County	District 19, Chair	Present	
Jason Bergeron	Chippewa County	District 7, Vice-Chair	Present	
Peter Gehring	Chippewa County	District 4	Present	
Charles Bomar	Chippewa County	District 12	Present	
Joel Seidlitz	Chippewa County	District 9	Present	

Others Present: Andy Albarado, Traci Bremness, Toni Hohlfelder, Leah Simington, Andy Bauer, Todd Pauls

3. MEMBERS OF THE PUBLIC WISHING TO BE HEARD

4. CONSENT AGENDA

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Peter Gehring, District 4
SECONDER:	Charles Bomar, District 12
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz

1. Approve the Agenda

2. Approve the Minutes

   Executive Committee - Regular Meeting - Sep 2, 2025 4:00 PM

3. Schedule Next Meeting Date - October 7, 2025

5. REPORTS

6. BUSINESS ITEMS

1. HIPPA Policy Revisions - Toni Hohlfelder
   Hohlfelder explained the revisions to the HIPPA policies are needed because we are a Business Associate and this will make us compliant.

RESULT:	**FORWARD TO COUNTY BOARD [UNANIMOUS]**	**Next: 10/14/2025 6:00 PM**
MOVER:	Joel Seidlitz, District 9	
SECONDER:	Jason Bergeron, District 7, Vice-Chair	
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz	

7. UPDATES, ANNOUNCEMENTS, AND CORRESPONDENCE

A. County Board Chair Report

B. County Administrator Operation Report

1. Update on FY26 Budget - Andy Albarado
   Albarado gave a preliminary review of the FY26 budget and explained they are still waiting for a few numbers before everything is finalized. At this time, the proposed tax rate is $2.13. The County's Equalized Value for FY26 increased by 10.39% or $990,587,300. The proposed property tax levy for the 2026 Chippewa County budget will increase to $22,393,725 from $21,713,416 from the 2025 budget. Overall, the property tax levy will increase by $680,309 or 3.13%.

   The Elder Benefit Specialist position that was previously approved will most likely not be filled. The preliminary numbers indicate there is not enough funding from the state to cover it.

RESULT:	**DISCUSSED**

8. AGENDA ITEMS FOR FUTURE CONSIDERATION

9. ADJOURN

The meeting adjourned at 4:19 p.m.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Joel Seidlitz, District 9
SECONDER:	Charles Bomar, District 12
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz

CHIPPEWA COUNTY

EXECUTIVE COMMITTEE

REGULAR MEETING

SEPTEMBER 2, 2025

CHIPPEWA COUNTY COURTHOUSE, RM 302

4:00 PM

1. CALL TO ORDER

Chair Hull called the meeting to order at 4:00 p.m.

2. ROLL CALL

Attendee Name	Organization	Title	Status	Arrived
Chuck Hull	Chippewa County	District 19, Chair	Present	
Jason Bergeron	Chippewa County	District 7, Vice-Chair	Present	
Peter Gehring	Chippewa County	District 4	Present	
Charles Bomar	Chippewa County	District 12	Present	
Joel Seidlitz	Chippewa County	District 9	Present	

Others Present: Andy Albarado, Traci Bremness, Toni Hohlfelder, Leah Simington, Todd Pauls, Brady Seidlitz, Mary Nelson, Jordan Hallingstad, Paul Brenner, Bobbie Jaeger, Andy Bauer, Travis Hakes

3. MEMBERS OF THE PUBLIC WISHING TO BE HEARD

4. CONSENT AGENDA

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Charles Bomar, District 12
SECONDER:	Peter Gehring, District 4
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz

1. Approve the Agenda
2. Approve the Minutes

   Executive Committee - Regular Meeting - Aug 19, 2025 4:00 PM
3. Schedule Next Meeting Date - September 16, 2025

5. REPORTS

1. Finance Update (2nd Quarter) - Leah Simington

   Simington reviewed the second quarter financials.

RESULT:	**REVIEWED**	**Next: 9/9/2025 6:00 PM**

6. UPDATES, ANNOUNCEMENTS, AND CORRESPONDENCE

A. County Board Chair Report

B. County Administrator Operation Report

1. County Board Supervisor Contact Information on New County Website - Andy Albarado
   Albarado explained the County is in the process of implementing a new website and asked for guidance from the committee on the amount of personal contact information that should be included on our new website for County Board Supervisors. The committee agreed to include their personal phone number and county email address.

RESULT:	**DISCUSSED**

7. BUSINESS ITEMS

1. Resolution to Establish Health Insurance Plan Funding for 2026 - Andy Albarado
   Albarado explained his recommendation for 2026 is to change the health insurance plan design from a two-tiered structure to a four-tiered structure and to establish employee premium contributions as follows: $30 for single, $150 for employee plus spouse, $124 for employee plus child(ren) and $212 for family. The HRA amount and the actual plan design is staying the same.

RESULT:	**FORWARD TO COUNTY BOARD [UNANIMOUS]**	**Next: 9/9/2025 6:00 PM**
MOVER:	Charles Bomar, District 12	
SECONDER:	Jason Bergeron, District 7, Vice-Chair	
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz	

2. The Executive Committee will convene in Closed Session pursuant to Wisconsin State Statutes Sec. 19.85(1)(g) "Conferring with legal counsel for the governmental body who is rendering oral or written advice concerning strategy to be adopted by the body with respect to litigation in which it is or is likely to become involved." (Confer with attorney and take possible action on tentative settlement in Rolling Hills Equine, Inc. v. Western Region Recovery and Wellness Consortium).
   The committee convened to closed session at 4:35 p.m. The following individuals were present: Andy Albarado, Leah Simington, Todd Pauls, Brady Seidlitz, Traci Bremness, All County Board Supervisors, Outside Insurance Defense Counsel from Crivello, Nichols & Hall, Staff representatives from Chippewa County DHS and WRRWC.

RESULT:	**APPROVED [4 TO 1]**
MOVER:	Charles Bomar, District 12
SECONDER:	Peter Gehring, District 4
AYES:	Hull, Bergeron, Gehring, Bomar
NAYS:	Seidlitz

The Committee will reconvene to open session and continue with the agenda.
The committee reconvene to open session at 5:13 p.m.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Charles Bomar, District 12
SECONDER:	Peter Gehring, District 4
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz

8. AGENDA ITEMS FOR FUTURE CONSIDERATION

9. ADJOURN

The meeting adjourned at 5:14 p.m.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Charles Bomar, District 12
SECONDER:	Joel Seidlitz, District 9
AYES:	Hull, Bergeron, Gehring, Bomar, Seidlitz

Department of Administration
Human Resources Division

September 16, 2025

TO: Executive Committee and County Board

FROM: Toni Hohlfelder

RE: HIPAA related policy updates

The following policies have minor updates related to Chippewa County being a Business Associate as the lead county for the Recovery and Wellness Consortium (RWC). At the time the policies were brought forward to the County Board, the consultant was not aware that Chippewa County was a Business Associate.

- Business Associate Policy
- Incidents Policy
- HIPAA Applicability and Organizational Requirements

The IT Policy was also updated due to being a Business Associate. In addition, Andy Bauer is making several policy recommendations located on page 18 of the IT Policy Manual related to Microsoft Teams and virtual meeting platforms.

Toni M. Hohlfelder, SHRM-CP, PHR

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

* PROPOSED REVISIONS *
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) and organizations for whom County is their BA.

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 and/or Covered Entity, 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 or County 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

e~~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/Subcontractors.

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. When the County serves as a BA to another organization and when providing services for that organization which involves the access, acquisition, use, or disclosure of PHI and/or ePHI:

a. The Department Head or designee shall educate applicable Workforce on what services may be provided, as described in the BAA.

b. Workforce shall follow the applicable Privacy, Security and Breach Notification Rule provisions, as well as the requirements of that organization's BAA. At minimum, Workforce shall:

1. Follow County's privacy and security policies, unless the BAA includes more stringent requirements workforce are required to follow.

2. Access, use, disclose, and request the minimum necessary PHI for assigned job responsibilities only as permitted or required by the BAA or required by law.

3. Report privacy and security incidents and breaches of confidentiality as outlined in the Incidents (Privacy & Security Incident Response, Breach Notifications, and Corrective or Disciplinary Actions) policy.

4. Provide clients, consumers, and their legal personal representatives access to the Designated Record Set (legal health record), as outlined in BAAs (including the ability to provide an electronic copy).

5. Provide Covered Entities with access to ePHI as outlined in BAAs and service level agreements.

6. Make PHI available for amendment and incorporate any amendments to PHI as requested by patients (and their legal personal representatives) and Covered Entities, as outlined in BAAs, as well as make changes to PHI as requested by Covered Entities as outlined in BAAs.

7. Document the date, name and address of the recipient, description of the PHI disclosed, purpose of the disclosure. This is to assist a Covered Entity in providing an accounting of disclosures to clients and consumers (and their legal personal representatives). The Department Head or designee shall facilitate providing accounting of disclosures to the Covered Entity / Individual as outlined in BAAs.

c. The Privacy Officer and/or Security Officer shall facilitate releases to the Secretary, as required by HIPAA to investigate or determine compliance with HIPAA.

d. Corporation Counsel, the Department Head or their designee shall facilitate the return (or destruction) of PHI to the Covered Entity at termination of the contract. If this is not feasible, notify the Covered Entity and continue to protect the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

~~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 or County and the Covered Entity, 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 / Covered Entity destroys, disposes or sanitizes the PHI and/or ePHI, obtain written notification from the BA / Covered Entity this was done.

    b. If returning, destroying, disposing or sanitizing is not feasible, request the BA / Covered Entity 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 / Covered Entity

    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

* PROPOSED REVISIONS *
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 and applicable Business Associate Agreements in place.

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. Refer to Business Associate Agreements and service level agreements for HIPAA notification requirements with Covered Entities. 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:

When the County is the Business Associate of another organization(s) and an incident resulted in a Breach of Unsecured PHI of that organization's PHI:

a). Provide notification to the Covered Entity(s) within the timeframe and to the privacy and/or security contact as required in the signed Business Associate Agreement (BAA).

1). If not specified, provide the notification without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach by the organization.

2). If an Agent of the other organization, provide the notification within 3 business days, whenever possible.

3). Do not delay initial notification to the other organization in order to collect all information needed for notifications.

b). Include the notification as much information as available at the time of the notification, including but not limited to the following:

1). A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, as well as how it happened, if known.

2). Identification of each individual whose Unsecured PHI was, or is reasonably believed to have been acquired, Accessed, used, or Disclosed in an unauthorized manner.

3). 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).

4). The identity, if known, of any individual who received PHI due to an unauthorized use or disclosure.

5). Any suggested steps the individual should take to protect themselves from potential harm resulting from the Breach.

6). A brief description of what the actions the County is taking to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches.

7). Contact information for questions and requests for additional information.

8). Any other available information that the other organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

c). The Covered Entity, not the County, is responsible for making the required notifications to Individuals, the media, and the Secretary of HHS.

1). Verify the Covered Entity will provide these required notifications.

2). The Privacy Officer may assist with providing these notifications only if requested by the Covered Entity, or Business Associate for whom the County is a Subcontractor.

~~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

* PROPOSED REVISIONS *
HIPAA APPLICABILITY AND ORGANIZATIONAL REQUIREMENTS

Purpose

Portions of Chippewa County are required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and modifications made to HIPAA, such as those made under the HIPAA Final Omnibus Rule (January 25, 2013), as well as other applicable privacy, security, and breach notification federal or state laws. The purpose of this policy is to define how, why, and what portions of the organization are required to comply with HIPAA. It also describes related overarching organizational requirements.

Responsible for Implementation

The Privacy Officer and Security Officer are responsible for implementing and overseeing this policy and procedure.

Policy

1. It is the policy of Chippewa County (herein County) to analyze and define how the organization needs to comply with HIPAA as applicable to the organization's general infrastructure/framework.

2. County designates itself as a Hybrid Entity. Although County is responsible for HIPAA oversight, compliance, and enforcement requirements, as applicable, the HIPAA Rules and County's HIPAA privacy, security, and breach notification policies and related procedures apply only to County's designated Health Care Components.

Procedures

1. As defined under HIPAA, Chippewa County is not:

   a. A Health Care Clearinghouse

   b. ~~A Business Associate and/or Subcontractor~~

   ~~c~~b. A part of an Affiliated Covered Entity

   c~~d~~. Participating in an Organized Health Care Arrangement (OHCA).

2. As defined under HIPAA, Chippewa County is a Business Associate and a Hybrid Entity.

   a. The County has designated certain components as Health Care Components, as defined by HIPAA, based on the following factors:

      1. The Health Care Component would meet the definition of a Covered Entity if it were a separate legal entity.

2. The Health Care Component would meet the definition of a Business Associate if it was a separate legal entity.

3. Services performed are Covered Functions.

b. Health Care Components:

1. The following Health Care Components meet the definition of a Health Care Provider type of Covered Entity as defined under HIPAA:

a). Department of Human Services and Public Health Department when providing clinical services that are electronically billed to a payor such as Medicare and Medicaid as a HIPAA health care claim or transmit any other Protected Health Information (PHI) in electronic form in connection with another HIPAA transaction.

b). Examples of these services provided by the Department of Human Services and Public Health Department may include: crisis intervention, medication management, psychiatric services, vaccinations, tuberculosis case management, lead visits, prenatal care coordination, reproductive health visits, etc.

2. The County Health Plan(s) also meets the definition of a Health Care Component, in its capacity of providing a self-insured health plan (a Group Health Plan) to its employees.

3. Due to the support services provided by the following roles to County's Health Care Component(s) listed above, they are also considered a part of the County Health Care Components:

a). Security Officer;

b). Privacy Officer;

c). Corporation Counsel Division;

d). Human Resources Division;

e). Information Technology Division;

f). Facilities & Parks Division;

g). Finance Division;

h). County Administrator; and

i). County Clerk.

c. Non-Health Care Components of the County include:

1. Aging and Disability Resource Center (ADRC) Division;
2. Child Support Department;
3. Clerk of Courts;
4. Coroner;
5. Criminal Justice Services Division;
6. District Attorney's Office;
7. Department of Administration (except as specified above);
8. Economic Support Division;
9. Emergency Management Department;
10. Highway Department;
11. Land Conservation and Forest Management Department;
12. Planning and Zoning Department;
13. Public Health nursing services that are funded by tax levy, and grant dollars such as CDC and DHS funding [as defined by WI State Statute(s) (e.g. 95, 250, 251, 252, 253, 254, and 255) and DHS Administrative Code(s) (e.g. 139, 140, 142, 144, 145, and 146)], and no HIPAA transactions are transmitted. Examples may include food safety and recreational licensing, human health hazards, communicable disease, chronic disease prevention, injury prevention, etc.
14. Register in Probate;
15. Register of Deeds;
16. Sheriff;
17. Treasurer;
18. UW Extension Department; and
19. Veterans Department.

3. As defined under Wisconsin Chapter 146 (146.81), Chippewa County is also a health care provider when providing Public Health nursing services:

a. When transmitting any health information in electronic form in connection with a HIPAA transaction, County is a HIPAA defined Health Care Provider as indicated above.

b. When no health information is transmitted in electronic form in connection with a HIPAA transaction (i.e. non-HIPAA Public Health nursing services), County:

1. Does not implement all of the HIPAA privacy, security, and breach notification policies, procedures, forms, or training program.

2. Follows Wisconsin Chapter 146 and other healthcare and public health related Wisconsin statutes.

4. For purposes of HIPAA privacy and security policies and procedures the above stated Health Care Components and Public Health nursing services are identified as "County," unless otherwise delineated.

5. Health Care Component(s) / Public Health nursing services / County in its capacity as a Business Associate of another Covered Entity shall not Disclose Protected Health Information (PHI) to a non-Health Care Component of the organization (treat the non-Health Care Component as a separate and distinct legal entity).

6. Health Care Components / Public Health nursing services / County in its capacity as a Business Associate of another Covered Entity shall protect electronic Protected Health Information (ePHI) and treat the non-Health Care Component as a separate and distinct legal entity.

7. If a Workforce Member performs duties for a Health Care Component / Public Health nursing services / County in its capacity as a Business Associate of another Covered Entity and non-Health Care Component of the organization, the Workforce Member shall not Use or Disclose PHI created or received in the course of or incident to the Workforce Member's work for the non-Health Care Component unless allowed by law.

8. Chippewa County shall create privacy and security policies and procedures and implements safeguards for the Health Care Components / Public Health nursing services / County in its capacity as a Business Associate of another Covered Entity to follow.

9. In an effort to achieve compliance with HIPAA regulations, Chippewa County has privacy, security, and breach notification policies, procedures, forms, and a training program in place. Chippewa County:

a. Performs multiple covered "functions" as defined under HIPAA (e.g. is a Health Plan, ~~and~~ Health Care Provider and Business Associate). The policies, procedures, forms, and training program are tailored as appropriate to comply with HIPAA as applicable to each "function" of the organization.

b. Does not maintain a facility directory, as defined under HIPAA and, therefore, is not required to have procedures in place for the facility directory provisions.

c. Does not sell PHI, as defined under HIPAA and, therefore, is not required to have procedures in place for the Sale of PHI provisions.

d. Does not use and disclosure PHI for marketing purposes as defined under HIPAA and,

therefore, is not required to have procedures in place for the marketing of PHI provisions.

e. Does not use or disclose PHI for fundraising purposes (for its own or any other Covered Entity's benefit) as defined under HIPAA and, therefore, is not required to have procedures in place for fundraising communication provisions.

f. Does not de-identify PHI or Use or Disclose de-identified PHI, as defined under HIPAA and, therefore, is not required to have procedures in place for the Use or disclosure of de-identified PHI provisions.

g. Does not Use PHI to create a Limited Data Set and/or does not use and disclose Limited Data Sets, as defined under HIPAA and, therefore, is not required to have procedures in place for the use or disclosure of Limited Data Set provisions.

h. Does not Use or Disclose PHI for research purposes as defined under HIPAA and, therefore, is not required to have procedures in place for the research of PHI provisions.

i. Is not a Health Care Clearinghouse, and therefore, does not have nor need any Health Care Clearinghouse procedures.

10. As a Business Associate, the County shall:

a. Follow policies and procedures provided to County Workforce by that organization, to the extent appropriate for services provided to an organization.

b. Forward requests for access and amend a Designated Record Set, restrictions, confidential communications, and accounting of disclosures to the applicable Covered Entity who owns the information subject to the request, unless is it the contractual responsibility of the County to facilitate.

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 document.

Resources

Entities Covered by the HIPAA Privacy Rule presentation, US Department of Health & Human Services, 2003: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/coveredentities.pdf

Applicable Standards/Regulations

- HIPAA Final Omnibus Rule, January 25, 2013
- 45 CFR § 160.102 Applicability

- 45 CFR § 160.103 Definitions
- 45 CFR § 164.104 HIPAA Privacy Rule Applicability
- 45 CFR § 164.105 HIPAA Privacy Rule Organizational requirements
- 45 CFR § 164.105(a) HIPAA Privacy Rule Health Care Component
- 45 CFR § 164.105(b) HIPAA Privacy Rule Affiliated Covered Entities
- 45 CFR § 164.105(c) HIPAA Privacy Rule Standard: Documentation
- 45 CFR § 164.106 HIPAA Privacy Rule Relationship to other parts
- 45 CFR §164.308(a)(4)(ii)(A) HIPAA Security Rule Isolating Healthcare Clearinghouse Function
- 45 CFR § 164.500 Applicability
- 45 CFR §164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes
- 45 CFR §164.502(a)(5)(ii) Sale of PHI
- 45 CFR §164.502(d) Uses and disclosures of de-identified PHI
- 45 CFR §164.504(f) Requirements for group health plans
- 45 CFR §164.504(g) Requirements for a covered entity with multiple covered functions
- 45 CFR §164.508(a)(3) Uses and disclosures for with an authorization is required – Authorization required: marketing
- 45 CFR § 164.510(a) Use and disclosure for facility directories
- 45 CFR §164.514(a) De-identification of PHI and §164.514(c) Re-identification
- 45 CFR §164.514(e) Limited data set
- 45 CFR §164.514(f) Fundraising communications
- 45 CFR §164.514(h) Verification requirements
- Wis. Stat. §146 Miscellaneous Health Provisions, 1/1/15
- Wis. Stat. §51.30 Mental Health Act, 1/1/15
- WI Stat. §95 Animal Health
- WI Stat. §250 Health; Administration and Supervision
- WI Stat. §251 Local Health Officials
- WI Stat. §252 Communicable Diseases
- WI Stat. §253 Maternal and Child Health
- WI Stat. §254 Environmental Health
- WI Stat. §255 Chronic Disease and Injuries
- DHS Administrative Code 139 Qualifications of Local Health Professionals Employed by Local Health Departments
- DHS Administrative Code 140 Required Services of Local Health Departments
- DHS Administrative Code 142 Access to Vital Records
- DHS Administrative Code 144 Immunization of Students
- DHS Administrative Code 145 Control of Communicable Diseases
- DHS Administrative Code 146 Vaccine-Preventable Diseases

*** PROPOSED REVISIONS ***

Chippewa County
Department of Administration
Information Technology Division

Information Technology Policy Manual

County Board History/Action
Adopted by the County Board December 10, 2019
Revised and Approved by the County Board 11/08/2022, 01/09/2024

Table of Contents

1. Information Privacy and Security Policy

Purpose

The purpose of this policy is to maintain the Confidentiality, Integrity, and Availability of all Protected Health Information (PHI), Electronic Protected Health Information (ePHI), restricted information and sensitive information (collectively Confidential Information) the organization creates, receives, maintains, and/or transmits. The purpose of this policy is to also have in place appropriate development, implementation, and oversight of the organization's efforts toward compliance with the HIPAA Privacy, Security, and Breach Notification Rules and continuously monitor privacy and security policies, procedures, and existing measures, and update them as needed to better protect Confidential Information.

Responsible for Implementation

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

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.

Policy

1. Supervision of Workforce and other information users

   It is the responsibility of all Department Heads, directors, elected officials, managers, supervisors, Privacy Officer, and Security Officer to supervise Workforce members and any other users of the organization's Confidential Information, systems, applications, servers, workstations, etc. Their responsibilities include, but are not limited to the following:

   a. Take all reasonable steps to make sure Workforce members and other users follow the organization's privacy and security policies and procedures and report non-compliance.

   b. Report non-compliance.

   c. Participate in incident investigations, as needed.

   d. Ensuring access to Confidential Information is the Minimum Necessary to complete job responsibilities.

   e. Request and provide only appropriate role-based, Minimum Necessary access to Confidential Information.

f. Monitor Workstations, systems, applications, and facilities for unauthorized use, tampering, and theft.

g. Employing measures to prevent the unproductive, inappropriate, or harmful use of information assets or systems.

2. Reporting and Compliance

a. All Workforce members and other users are required to report non-compliance of the organization's privacy and security policies and procedures to the Privacy Officer or Security Officer (refer to the Incidents policy).

b. Workforce members have the responsibility of assuring the privacy and security of Confidential Information.

c. Individuals that exercise their rights and/or report violations may not be subjected to intimidation, threats, coercion, harassment, discrimination against, or any other retaliatory action as a consequence.

d. Violation of any privacy and/or security policy, procedure, standard, law and/or regulation:

1. By Workforce members may result in disciplinary action, up to and including termination of employment.

2. By others, including Business Associates and partners may result in termination of the relationship and/or associated privileges.

3. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations. Personal legal liability continues after employment or a business relationship ceases with the County.

e. The County reserves the right to notify law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

f. The County does not consider conduct in violation of this and/or any other privacy and security policies and procedures to be within a Workforce member's, Business Associates', or partner's course and scope of employment or partnership, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, the County reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

g. If a Workforce member, Business Associate, or partner believes he or she has been requested to undertake an activity which he or she believes is in violation of this and/or any other privacy and/or security policy and procedures, he or she must provide a written or verbal complaint to the Privacy Officer or Security Officer or any Department Head as soon as possible.

3. Privacy and Security Incident Response

a. Detection and Reporting

1. Clients, consumers, subscribers, and other individuals may report complaints concerning the County's patient 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, other system users, and Business Associates are required to report non-compliance of the organization's privacy and security policies and procedures to the Privacy Officer and/or Security Officer through an internal email or direct phone call.

3. Immediately upon observation of suspected and known privacy and security violations, Precursors, Indicators, Security Incidents, Privacy Incidents, and Breaches:

a). Workforce members, system users, Business Associates, and other Vendors are required to report them to the Privacy Officer and/or Security Officer through an internal email or direct phone call.

b). In the absence of the Privacy Officer and/or Security Officer, or in the event of the Privacy Officer and/or Security Officer involvement report the incident directly to a Department Head.

b. Investigation and Sanctions

1. Individuals that report privacy and security issues, complaints, breaches, and violations in good faith, or testifies or participates in an investigation, compliance review, proceeding, or hearing may not be subjected to intimidation, threats, coercion, harassment, discrimination against, or any other retaliatory action as a consequence. This includes reports made to the County and/or appropriate regulating bodies.

The County may not require individuals to waive their legal rights to complain as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

2. The Privacy Officer and/or Security Officer or designee promptly facilitates a thorough investigation of all reported privacy and security violations and incidents, including Breaches, and documents the investigation actions taken. Facts concerning the breakdown in job performance or lack of adherence to established work rules are obtained and considered.

Investigation assistance may be requested from Workforce and other system users.

All individuals are required to cooperate with the investigation process and provide factual information.

Internal as well as federal and state investigations and disciplinary proceedings: All Workforce are required to cooperate with the investigation process and provide factual information. Workforce may not interfere with investigations or disciplinary proceedings by willful misrepresentation or omission of facts or by the use of threats or harassment against any person. Whether it was intentional or non-intentional, individuals suspected of non-compliance of the Privacy Rule, Security Rule, and/or the organization's privacy and security policies and procedures are provided the opportunity to explain their actions.

Care shall be taken to ensure that the results of investigations are disclosed only to a Department Head and other leaders involved in any investigation and that information which may further expose organizational risk is shared with extreme caution.

Breach risk assessments and notifications are facilitated by the Privacy and/or Security Officer.

3. Individuals being investigated are not informed that they are being investigated until evidence is provided that indicates a privacy or security policy has been violated, unless it is necessary to inform them in order to make this determination.

c. Sanctions

1. Fair, impartial, and consistent levels of sanctions, such as disciplinary action, are provided based on the type and magnitude of harm that resulted in the violation, prior performance reviews and non-compliance, previous education provided, relevant legislations, as well as whether it was intentional or non-intentional by the Human Resources Director.

a). Sanctions provided are intended to correct behavior, re-instill the incentive for self-corrective action, and preserve the discipline of the entire department or organization.

b). Sanctions may be provided to Workforce and vendors, contractors, and other service providers.

2. Refer to Chapter 6 (Employee Conduct) of the HR Policy Manual for examples of sanctions that may be provided.

4. Facility Access Controls

a. Workforce members must approach individuals in Restricted Areas that are not being escorted by a Workforce member by stating, "May I help you?", unless they feel

unsafe to do so. Keep in mind the individual may be a consumer, client, subscriber, Vendor, or intern.

1. Escort violators of this policy and procedure out of Restricted Areas immediately and escort them to the area in which they are trying to go.

2. If Workforce members feel unsafe to approach the individual, they are required to immediately report the situation to the Department Head or Supervisor.

b. All Workforce members are responsible for reporting a potential or known incident of unauthorized visitor, unauthorized access to the organization's facility(s) and/or areas containing information systems that create, receive, maintain, and/or transmit Confidential Information and/or physical security access control issues or incidents as described in the Privacy and Security Incident Response procedures.

c. Securing Confidential Information within the facilities.

1. Confidential Information may not be left unattended in Unrestricted Areas.

2. Erase whiteboards containing Confidential Information before leaving Unrestricted Areas.

3. Client, consumer, and subscriber photographs, letters, cards, may not be visible at any time.

4. Hard copy (e.g. printed) documents containing Confidential Information in Restricted Areas:

a). Are turned over, covered up, or put away when unattended during working hours so they cannot be viewed by a passerby (including other co-workers)

b). May not be stored in unlocked or in unsecure containers or open workspaces when unattended.

c). Are removed from printers and copiers and secured after being printed.

d). Are removed from fax machines and distributed to the appropriate recipients several times throughout the day.

5. At the conclusion of the workday Workforce shall ensure that their workspace is clear of all client, consumer, subscriber, and other identifying information (this includes names, telephone numbers, etc., both personal and professional). This also includes client files, notes, post-its, etc. Files shall be placed in the record file room or a file cabinet or desk drawer in the Workforce member's workspace area. Workforce shall close and lock suite

doors that provide access to Restricted Areas. Workforce are highly encouraged to close and lock office doors.

6. Medical record file rooms are locked when unattended, except when being used during the day.

   a). Access is limited to the minimum necessary Workforce.

   b). Maintain Treatment Facilities records in a secure manner to prevent unauthorized access (note: this is required for Treatment Facilities (treatment of Alcoholic, Drug Dependent, Mentally Ill or Developmentally Disabled persons) under WI DHS 92.03(1)(k).

   c). Maintain records of patients diagnosed or received treatment for alcohol or drug abuse at a federally assisted program in secure rooms, locked file cabinets, a safe or other similar container when not in use (note: this is required by 42 CFR part 2, 2.16).

   d). Once a client record is closed, the file shall be returned and maintained in the designated file room.

d. Individuals issued with facility keys, ID badges, access devices, and cypher codes:

1. May not share them with any other individual. Exceptions are approved and documented by the Human Resources Division and Facilities & Parks Division.

2. May not permit access to individuals not authorized to enter the building(s) and room(s).

3. May only use them to enter the organization's building(s) and rooms to complete job responsibilities for the organization.

4. Are required to secure them so they are not accessible to unauthorized individuals.

5. Are required to immediately report when they are lost, stolen, or otherwise compromised to the Human Resources Division, Facilities & Parks Division or Department Head who facilitates the following:

   a). Changes the lock or deactivates the cypher code, ID badges, access devices.

   b). Initiates an incident report as described in the Privacy and Security Incident Response section.

6. Are required to return them to the Human Resources Division, Supervisor or Department Head:

   a). When no longer needed

b). On their last day of employment or contracted work.

e. To protect resources, including Confidential Information, when the following offices are unattended and/or closed, the doors are closed and locked:

1. Chippewa County Department of Human Services (CCDHS)

2. Chippewa County Department of Public (CCPDH)

f. Exterior building doors may not be unlocked and/or be propped open and left unattended after business hours. Exceptions are reviewed, approved or denied, and documented by the Human Resources Division and Facilities & Parks Division.

g. Refer to the following policies for additional facility access or security related control requirements:

1. Facility Use Policy

2. Facility Access and Physical Security Policy

3. Key Issuance and Request Policy

4. Identification and Access Card Policy (located in the HR Policy Manual)

5. Facility Maintenance

a. Before making any Repair and Change to a department that may impact the privacy and security of Confidential Information, forward plans to the Privacy Officer and/or Security Officer to review and approve them.

b. Refer to the Facility Maintenance Policy for additional requirements.

6. Vendor / Contractor Services

a. Business Associate Agreements (BAA). 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 PHI or ePHI, contact the Corporation Counsel Division to assess whether a BAA is needed. A signed BAA is obtained before allowing the BA to acquire, access, use, or disclose PHI or ePHI. The Corporation Counsel Division also works with Covered Entities to review and sign BAAs with them.

b. As part of the County's effort to utilize service providers with a high level of privacy and security controls in place, 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, contact the IT Division / Security Officer. The IT Division / Security Officer facilitates

validating privacy and security controls and service contracts are appropriate for the types of services being provided.

c. Refer to the Business Associate and Service Provider policies for additional requirements for Business Associates and other third parties.

7. Disposal of Confidential Information

a. Confidential Information is destroyed/disposed/Sanitized using a method that ensures the Confidential Information cannot be recovered or reconstructed

b. Workforce members and Business Associates (BAs) are responsible for collecting, identifying, and segregating all types of all Confidential Information on behalf of the organization.

c. Media containing Confidential Information may not be directly disposed of in a garbage can, dump, or landfill.

d. Confidential Information and other records and types of information may not be disposed of prior to meeting minimum retention periods established in the Chippewa County Code of Ordinances Chapter 3 – Records Retention. Workforce and other users are required to follow the County's Information Retention policies.

e. Client, consumer, and subscriber records are not destroyed, disposed or Sanitized if they are known to be, or if there is a potential for them to be, involved in any open investigation, audit or litigation.

1. Destruction, disposal or Sanitization is suspended for these records until such time as the situation has been resolved.

2. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order is obtained to ensure that the records are returned to the organization or properly destroyed/disposed/Sanitized by the requesting party.

f. When Electronic Media is no longer needed, forward it to the IT Division to securely dispose of it.

g. Disposal of paper records: Copies of documents and images that contain Confidential Information which are not originals and that do not require retention based on retention policies (e.g., provider copies, schedule print outs, etc.).

1. Place them in locked bins designated for shredding when ready for disposal. Workforce who have a confidential disposal container at their workstation shall empty the container into the locked bins designated for shredding by the end of each workday.

2. Documentation of this type of disposal is not required, unless done by a contracted organization.

3. Contracted Vendors shred or destroy documents so that the Confidential Information cannot be read or otherwise cannot be reconstructed; redaction is specifically excluded as a means of data destruction. An example is to finely shred papers.

h. Copies of client, consumer, subscriber designated record sets (e.g. medical charts, billing files, etc.):

1. Only the Department Head or designee for the designated record set may facilitate destruction of these records.

2. Refer to the Chippewa County Code of Ordinances Chapter 3 – Records Retention or other Department procedures for retention requirements.

8. Reuse of Electronic Media Containing Confidential Information

a. 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), forward it to the IT Division to facilitate removal of all Confidential Information and/or makes it inaccessible, cleaned, or scrubbed.

b. When a contracted vendor disposes of Electronic Media, obtain a certificate of destruction.

9. Privacy and Security Training

The County's privacy and security training program is required for all Workforce members.

Resources

NIST Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, revision 4, April 2013

Applicable Standards / Regulations

- HIPAA Final Omnibus Rule, January 25, 2013
- 45 CFR § 160.103(a) HIPAA definition of Electronic Media (1/25/13)
- 45 CFR §164.308(a)(1)(ii)(c) HIPAA Security Rule Sanction Policy
- 45 CFR §164.308(a)(3)(ii)(A) HIPAA Security Rule Authorization and/or Supervision
- 45 CFR §164.308(a)(5)(i) HIPAA Security Rule Security Awareness and Training
- 45 CFR §164.310(a) HIPAA Security Rule Facility Access Controls
- 45 CFR §164.308(a)(4)(ii)(B) – HIPAA Security Rule Access Authorization
- 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 & Validation Procedures
- 45 CFR §164.310(a)(2)(iv) HIPAA Security Rule Maintenance Records
- 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. 164.530(e) HIPAA Privacy Rule Sanctions
- 45 CFR § 164.530(g) HIPAA Privacy Rule Refraining from intimidating or retaliatory acts
- 45 CFR §164. 164.530(h) HIPAA Privacy Rule Waiver of Rights
- Wis. HFS 92, Nov. 2008

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. <u>User Accounts and Passwords</u>

   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, Instant Messaging, Paging Via a Pager, and Overhead Paging

Texting, ~~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.

The County exclusively uses Microsoft Teams for all electronic communication, which ensures all communication is encrypted. Therefore, any instant messaging communication sent through Microsoft Teams is acceptable including ePHI and other Confidential Information. ePHI and Confidential Information shall not be sent through any other instant messaging system at any time, from any device.

12. Virtual Meeting Platforms

Microsoft Teams is the ~~O~~only virtual meeting platform~~s~~ managed by the IT Division that 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.

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

1. When needed to perform assigned job responsibilities
2. As allowed by County policies and procedures
3. As allowed by law

~~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~~.

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.

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.

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.

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.

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 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.

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.

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.

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.

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

(Amended by the County Board: 11-08-2022)

3. Mobile Device Management Policy

Purpose

The purpose of this policy is to define the responsibilities, guidelines, and terms of use for County issued devices or personal mobile devices configured to sync Chippewa County (herein County) email, calendar or contact data by providing a mobile device management (MDM) solution. The MDM solution provides the County with a means of performing an enterprise wipe of county data residing on the personal mobile devices as needed, encrypt the device, and require passcodes to be used to access the device.

Responsible for Implementation

The Information Technology Director and Human Resources Director are responsible for implementing and overseeing this policy.

Scope

This policy applies to all Employees that have a County issued device (smart phone or tablet) or a personal mobile device (smart phone only) configured with active sync to receive Chippewa County email, calendar or contact data and to create, receive, maintain, or transmit Confidential Information.

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.

Policy

1. County issued mobile devices:

    a. Upon approval of the County Administrator, some positions or employees may be authorized to use a County-issued smart phone.

    b. All County issued smart phones shall be setup with a County issued account provided by the Information Technology Division (including Apple IDs or other required applications).

    c. County issued devices are for business purposes only and shall not be used for personal use. Personal calls and texts are prohibited. Personal pictures or data are prohibited to be taken or stored on County issued devices.

    d. Even though County issued devices might be used away from County, the usage and service records are still public information. They are also subject to County inspection. The County reserves the right to access the contents, applications, communication records and messages on any device at any time. Employees are responsible for following all appropriate record retention rules.

    e. Wi-Fi settings shall be set to not automatically connect to unsecured networks. Extreme caution should be exercised in connecting to any unsecured or public access points.

    f. Employees shall not download any software onto a County-issued mobile device unless authorized by the Information Technology Division.

    g. Use of a County-issued mobile device outside of the continental United States or internationally is prohibited unless approved by the Information Technology Director or designee.

h. Prior authorization by the Department Head or designee is required for an employee to use a County-issued phone or tablet outside of non-work hours. Use of County-issued phones or tablets during non-work hours shall be recorded as compensable work time by non-exempt unless such time is de minimus (i.e. increments of time less than 10 minutes).

2. Personal Mobile Devices requirements:

a. Personal mobile devices may be approved by the Human Resources Director for exempt employees only. The Department Head or designee is responsible for authorizing the use of personal mobile devices to sync email, calendar and contact data only.

1. The Department Head or designee shall forward requests to the Human Resources Director or designee for approval.

2. The Human Resources Division shall forward the approved request to the Information Technology Division via the help desk ticketing system.

b. Information Technology responsibilities:

1. Configuring the authorized user's personal mobile device via active sync to receive and access Chippewa County email, calendar and contact data (Chippewa County data) and shall not create, receive, maintain, or transmit Confidential Information via any other means. Chippewa County will license only one (1) personal device for Chippewa County data for each Authorized user. Some exceptions may apply.

2. Setting up the MDM software on the device.

3. Device removal and performing a "remote wipe" of Chippewa County data from the authorized user's lost or stolen device.

4. Smartphone or tablet system removal and performing a "remote wipe" of Chippewa County data from an authorized user’s device upon termination of employment and/or certain discipline with Chippewa County.

c. MDM Authorized / Personal Mobile Device user responsibilities:

1. User is responsible for using Chippewa County email, and any other Confidential Information, on his or her personal device or County issued devices within the same constraints as all Chippewa County-owned device and adhering to all Chippewa County Information Technology Policies.

2. Users are required to report lost, misplaced or stolen personal equipment or workstations that are used to conduct County business and connected to the County MDM solution to the Security Officer and Information Technology Director.

3. Prior to trading in or selling an MDM Authorized Personal Mobile Device, the user shall bring the device to the Information Technology Director or designee for the MDM software to be removed from the device.

d. Personal Mobile Devices shall not be:

1. Configured for active sync of email, calendar or contacts or to create, receive, maintain, or transmit Confidential Information without being connected to the County MDM solution.

2. Connected to the County network in any way (i.e. via wired or wireless connection), unless set up by the Information Technology Division (the County's guest wireless access may be used).

3. Used to open County files from County-owned devices (e.g. flash drives, media tapes, backup drives, Workstations, etc.)

4. Utilized to record or document or download client, consumer, or subscriber information or Protected Health Information (PHI).

5. Utilized to download and/or store other types of Confidential Information on the device, unless as approved.

6. Utilized to take and/or send pictures of clients, consumers, or subscribers or their PHI. Pictures may not be taken in Restricted Areas or where PHI, or any client's, consumer's, or subscriber's identifiers (e.g. papers, charts, images, etc.) may be the background.

7. Utilized to take and/or to send pictures of confidential or sensitive information. This includes, but is not limited to, law enforcement investigations or crime scenes.

e. Personal Mobile Devices shall meet the County's security standards, including but not limited to the following:

1. Devices may not be "jailbroken" or have any software or firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

2. To jailbreak a mobile device means to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

3. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that the County's data is only sent through the County's email system. If a user suspects that company data has been sent from a personal email or other business email account, either in the body text or as an attachment, they must notify the Security Officer.

f. Users are responsible for obtaining their personal device as well as maintaining and paying any monthly or annual fee to the mobile carrier. All mobile charges that the user incurs are his or her responsibility, regardless whether such charges are work related or for personal use. This includes, but is not limited to, charges resulting from texts, data plan surcharges, calls, navigation, or application uses or from early termination fees.

g. Users are responsible for all personal mobile device support, including the cost of repairs or replacement.

Applicable Standards/Regulations

- 45 CFR §164.308(a)(3)(i) HIPAA Security Rule Workforce Security
- 45 CFR §164.308(a)(3)(ii)(C) HIPAA Security Rule Termination Procedures
- 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 §164.310(c) HIPAA Security Rule Workstation Security

4. 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. Data Backups – General Requirements

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

2. Confidential Information Data Backup

    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. Moving Confidential Information – Electronic Media

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:

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

(Adopted by the County Board: 11/08/2022)

5. 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

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

(Adopted by the County Board: 11/08/2022)

6. 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

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

(Adopted by the County Board: 11/08/2022)

7. 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, Bb~~b~~usiness Aa~~a~~ssociates, 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

- 45 CFR §164.308(a)(3)(i) HIPAA Security Rule Workforce Security
- 45 CFR §164.308(a)(3)(ii)(B) HIPAA Security Rule Workforce Clearance Procedures
- 45 CFR §164.308(a)(3)(ii)(C) HIPAA Security Rule Termination Procedures
- 45 CFR §164.308(a)(4)(i) HIPAA Security Rule Information Access Management
- 45 CFR §164.308(a)(4)(ii)(A) HIPAA Security Rule Isolating Healthcare Clearinghouse Function
- 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)(D) HIPAA Security Rule Password Management
- 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)(1) HIPAA Security Rule Access Control (Technical)
- 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(d) HIPAA Security Rule Person or Entity Authentication

(Adopted by the County Board: 11/08/2022)

8. **Technical Access Control:** Transmission Security, Encryption, and Integrity

Purpose

Electronic Protected Health Information (ePHI) and other Restricted Information and Sensitive Information (collectively "Confidential Information") are transmitted and stored in many different ways. Utilizing strong technical encryption and integrity mechanisms to secure this information helps to protect the confidentiality, integrity, and availability of it.

The purpose of this policy is to define methods to:

1. Prevent unauthorized access, use, disclosure, and modification of Confidential Information during transmissions over electronic communication networks.

2. Encrypt Confidential Information at rest and in transit, whenever possible and deemed appropriate to help protect the confidentiality, integrity, and availability of Confidential Information.

3. Prevent Confidential Information from being improperly altered or destroyed.

4. Have the ability to verify that Confidential Information is not improperly altered or destroyed.

Responsible for Implementation

The IT Director is responsible for implementing and overseeing this policy. It is the responsibility of the IT Division and Department Heads to ensure processes comply with this policy.

Policy

It is the policy of Chippewa County to:

1. Implement measures to prevent unauthorized access to Confidential Information during transmission over electronic communication networks.

2. Define how and when to implement mechanisms to securely encrypt and decrypt Confidential Information at rest and in transit, whenever feasible.

3. Outline procedures and implement technical methods to protect Confidential Information from improper and/or unauthorized alteration or destruction.

4. Establish electronic mechanisms and other security measures to ensure and validate that Confidential Information hasn't been altered or destroyed in an unauthorized manner until properly disposed.

Encryption and Other Mechanisms Used to Secure Confidential Information at Rest and In Transit

1. County considers methods to encrypt Confidential Information at rest and in transit, to assist in its efforts to prevent unauthorized access, alteration, and destruction.

2. The IT Director or designee completes a risk assessment to determine the need and ability to encrypt ePHI, as well as the type of encryption to use.

    a. Factors considered in the decision-making process include the cost, likelihood of loss or theft, likelihood of a breach of confidentiality, fines, ability to encrypt, loss of reputation, as well as other factors and/or negative impacts that may happen based on the decision.

    b. If it is determined that Confidential Information does not need to be encrypted, the IT Director:

        1. Completes an exception request, including documentation as to why it would not be reasonable and appropriate to implement the implementation specification (refer to the Privacy & Security Oversight Policy);

        2. Implements an equivalent alternative measure if reasonable and appropriate.

    c. If it is determined that the Confidential Information will be encrypted:

        1. The use of proprietary (custom) encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer. The export of encryption technologies is restricted by the U.S. Government.

        2. Use strong cryptography, such as the following, unless not available:

            a). A minimum of 256-bit encryption.

            b). Ciphers must meet or exceed the set defined as "AES-compatible".

                1). Utilize proven, standard algorithms such as the current Advanced Encryption Standard (AES).

                2). All ciphers in use are reviewed at least annually for deprecation. Threat intelligence or cipher deprecation may accelerate review or replacement.

            c). For data in transit comply with, as appropriate:

                1). Federal Information Processing Standards (FIPS) 140-2 validated.

                2). NIST Special Publication (SP) 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.

3). NIST SP 800-77, Guide to IPsec VPNs; or NIST SP 800-113, Guide to SSL VPNs.

d). For data at rest, encryption consistent with NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices

e). Users may not (refer to the Information Privacy and Security policy):

1). Share encryption keys or user names and passwords.

2). Leave them so someone else may see/find them.

f). Strong passwords are used when creating encryption passwords (at a minimum, randomly generated 36 characters).

g). Encryption Keys:

1). Are secured and stored in an encrypted format.

2). Only the minimum necessary IT Division Workforce has access to encryption keys. The IT Director approves all requests for encryption key custodians (also refer to the System Access policy).

3). Encryption key custodians are responsible for ensuring:

- Strong key generation.
- Keys are issued with an expiration date, whenever possible.
- Secure key distribution.
- Storage within a secure cryptographic device, such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device.
- Periodic key changes.
- Destruction of old keys, verified via an email to the IT Director.
- Prevention of unauthorized substitution keys.
- Replacement of known or suspected compromised keys.
- Destruction of old or invalid keys.
- Split knowledge and dual control key process to recover or reconstruct keys.
- Encryption key custodians acknowledge in writing or electronically that they understand and accept key custodian responsibilities.

4). Key-encrypting keys:

- Must be at least as strong as the data encrypting key.

- Are stored separately from data-encrypting keys and in the fewest possible locations.

5). Keys known or suspected to have been compromised are replaced immediately and an incident investigation is initiated as described in the Incidents policy and Privacy and Security Incident Response section of the Information Privacy and Security policy.

h). Encryption authentication

1). Use secure protocols for key exchanges (e.g. cryptographic protocols such as Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH)).

2). End points must be authenticated prior to the exchange or derivation of session keys.

3). Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash (e.g. secure hashing algorithm (SHA-2)).

4). Install a valid certificate signed by a known trusted provider for all servers used for authentication (for example, RADIUS or TACACS).

5). All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

i). Document the type of encryption utilized in the inventory list.

3. Workstations (computers, laptops, USB/Flash Drives, CDs, Smartphones, etc.; refer to the definition of a Workstation for a complete list)

a. The IT Division:

1). Installs BitLocker encryption Workstations before distributing them to users.

2.). Distributes smartphones distributed with native encryption activated (i.e. on iPhones).

3). Manages this encryption on Workstations and smartphones.

b. USB/Flash Drives may not be utilized to store Confidential Information.

c. Refer to the Confidentiality section of the Information Technology Policy Manual regarding storage of Confidential Information on a Workstation and any other portable device requirements.

4. Photocopiers, printers, fax machines and all-in-one devices, and Portal Breath Test (PBT) kiosk

a. Storage drives on these devices are encrypted.

b. This encryption is installed, managed, and monitored by the authorized contracted IT vendor.

c. The PBT is bolted or secured to a wall.

5. Servers and Backups

a. Servers, including cloud hosted / online storage, that contain Confidential Information are encrypted with full disk encryption or encrypted at rest (i.e. 256-bit AES; SAN volume encrypted where the server is stored).

b. Backups that contain Confidential Information are protected using encryption (e.g. full disk 256-bit AES).

c. Encryption on servers and backups is installed, managed, and monitored by the IT Division.

6. Emails

a. The IT Division installs, manages, and monitors the technology for users to encrypt emails and/or attachments.

b. Refer clients, consumers, and subscribers requesting a copy of their designated record set be emailed, as described in County release of information policies.

c. Refer to the Information Technology Policy Manual which outlines when and how to send encrypted emails.

d. Secure, encrypted emails track when an email has been opened by the recipient.

7. Texts, Instant Messages, Paging Via a Pager, and Overhead Paging. As per the Texting, Instant Messaging, Paging Via a Pager, and Overhead Paging section of the Information Technology Policy Manual, texts, instant messages, and pages may not currently include Confidential Information.

8. Virtual meeting platforms

a. The IT Division manages virtual meeting platforms, Webex, Zoom, and Microsoft Teams, which are approved to be used.

b. As per the Virtual Meeting Platforms section of the Information Technology Policy Manual:

1). Webex, Zoom, and Microsoft Teams may be used for internal workforce meetings, general internal communications, and scheduling meetings with vendors. Note: vendors and other organizations may send invitations to Chippewa County workforce utilizing their own platforms which may be utilized to attend virtual meetings.

2.) No virtual meeting platform may be used to transmit Confidential Information at any time, with the exception of telehealth services provided consistent with the Telehealth policy.

9. Network Transmissions (of Confidential Information to/from other entities/sites as well as internally)

a. Confidential Information is transmitted only when allowed by this policy and the County's release of information policies. Also, refer to the Information Technology Policy Manual.

b. External network transmissions of Confidential Information may only be done using one of the following methods which are installed, managed, and monitored or reviewed and approved by the IT Division or designee. Exceptions are reviewed, approved, and authorized by the Security Officer. The following are examples provided by County that may be used:

1). File Transfer Protocol over SSL (FTPS) with a protected communication path:

a). Secure Shell (SSH) to copy the data from one location to another; this method is generally referred to as Secure File Transfer Protocol (SFTP); and/or

b). Transport Layer Security (TLS) to protect the connection of a standard FTP transmission:

- Use TLS 1.2 or higher.
- Disable TLS 1.0, TLS 1.1, and SSL 1, 2, 3.x unless required. (Note: use of TLS 1.0, TLS 1.1, and SSL 1, 2, 3.x is leading to increased cases affected by Man-in-the-middle (MITM) attacks and session hijacks)

c). HTTPS.

2). Internet protocol security (IPSEC): minimum of 128-bit / SHA2 (e.g. SHA-256).

3.). Remote access through the Virtual Private Network (VPN) (private point-to-point network) via Fortinet: minimum of 256-bit SSL.

c. Only Workstations (including portable devices) authorized by the IT Division are allowed on County's network.

d. Unused network data jacks should be disabled in Unrestricted areas whenever feasible, to prevent non-organization devices to connect to the network County's knowledge. Visitors are escorted at all times in rooms and areas where network data jacks are active.

e. Conference room internal data network jacks are disabled to prevent non-organization devices to connect to the internal network without County's knowledge.

10. Wireless Access Points

a. The IT Division installs, manages, and monitors all wireless access points.

b. WPA2 or higher (EAP-TLS or PEAP authentication) is used for all non-public wireless access points. A strong password is utilized to access them (refer to the Technology and Information Privacy and Security; Unique User IDs, Passwords, and Configurations Policy; and System Access policies for minimum password requirements).

c. A separate, segmented guest wireless network is available for authorized personally owned devices (e.g. for employees and approved vendors).

d. A separate, segmented public wireless network is available for visitors' use. This public wireless network may not be used by Workforce to transmit Confidential Information, unless connected through the County VPN.

e. Only Workstations authorized by the IT Division are allowed on County's wireless network.

System Isolation

ePHI Information Systems are segmented from lower system classification and from non-ePHI systems such as:

1. HVAC systems and iOT devices.

2. When possible and applicable, test networks, systems, and applications are separated from production systems, either physically or through local access control list controls on the system.

3. Networks the IT Division does not manage are connected to only those systems with which they need to interface to conduct business, etc.

Integrity

Chippewa 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

of according to the Disposal of Confidential Information Policy. These include, but are not limited to the following:

1. Users may only change/amend Confidential Information in Information Systems and on their Workstations as described in County's policies and procedures.

2. Users, during the regular course of their job responsibilities, are required to check for and report any errors or potential errors involving Confidential Information identified in Information Systems.

3. Suspected and known data integrity issues are investigated and mitigated in accordance with the Incidents Policy.

4. The IT Division ensures that Information Systems are tested for accuracy and functionality before using them in the live environment. In addition, before integrating Confidential Information from one Information System into another, the data is validated.

5. While completing a risk analysis, County considers various risks to the integrity of Confidential Information and identifies security measures to reduce risks, as described in the Information Security Risk Management Policy.

6. Role based, minimum necessary access is authorized, and duties are segregated, as described in the System Access and Technology and Information Privacy and Security policies.

7. The following maintain an inventory / have the ability to identify in systems privileged access rights, indicating who has access to what, who has permission to do what, and the date when a document was last reviewed and updated.

    a. IT Division for Active Directory.

    b. System Administrators for other systems/applications.

8. Audit trails on Information Systems and Workstations are in place to identify all changes made to Confidential Information, as described in the Auditing and Technology and Information Privacy and Security policies.

9. Anti-virus/malware is installed and updated, as described in the Malicious Software Protections policy and Malware Standard.

10. Physical and technical security controls are in place to prevent unauthorized access to Workstations and Information Systems, as described in the and Technology and Information Privacy and Security; Information Privacy and Security; System Access; Facility Access (and Physical Security); Facility Use; Identification and Access Card; Key Issuance and Request Policy Changes; Facility Maintenance; and System Build/Change Control policies, procedures, and standards.

11. Encryption and other mechanisms to secure information, as described in this policy, are utilized to prevent transmission errors and unauthorized access to Confidential Information.

12. Whenever possible, a hashing algorithm with a security strength equal to or greater than SHA-2 (Secure Hash Algorithm) as specified by the NIST SP 800-131AR1 (November 2015) is utilized to verify that ePHI has not been altered.

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 document.

Resources

- HIPAA COW Encryption Whitepaper, 2010
- Office for Civil Rights "Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals"
- NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- NIST Special Publications 800-57, Recommendation for Key Management, Part 1: General
- NIST Special Publications 800-77, Guide to IPsec VPNs
- NIST Special Publications 800-113, Guide to SSL VPNs
- NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices
- NIST Special Publications 800-131AR1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November 2015
- FIPS 140-2 Standard, 5/25/01 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- FIPS 140-2, 7/25/13 Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf
- SANS Acceptable Encryption Policy, June 2014

Applicable Standards/Regulations

- 45 CFR §164.312(a)(2)(iv) HIPAA Security Rule Encryption and Decryption
- 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(c)(1) HIPAA Security Rule Integrity
- 45 CFR §164.312(c)(2) HIPAA Security Rule Mechanism to Authenticate Electronic PHI
- 45 CFR §164.312(e)(2)(i) HIPAA Security Rule Integrity Controls

(Adopted by the County Board 01/09/2024)

Department of Administration

Andy Albarado, County Administrator

September 10, 2025

TO: Executive Committee

FR: Andy Albarado

RE: County Administrator 2026 Proposed Budget Update

At the May County Board meeting, you received a presentation explaining the overall budget process. Throughout the summer, policy committees have been working on reviewing department-level budgets. In recent weeks, our new Finance Director, Leah Simington, and I have met one-on-one with each Department Head to better understand their operations and to identify potential savings and efficiencies. We are still awaiting the state's final shared revenue numbers, but other details for revenues are already known. This memo is intended to give you a brief overview of key elements involved in building the budget, ahead of my formal recommendation to the Executive Committee on October 7th.

Adopting the annual budget is among the most significant policy responsibilities you have as County Board Supervisors. Items such as resolutions for the Capital Improvement Program (CIP), tax levy allocations for salary adjustments, and health insurance are treated as preliminary placeholders during the budget-building process. These items do not become final until the full budget is approved in November.

NET NEW CONSTRUCTION

The net new construction percentage increase has been received. This percentage is multiplied by our net levy from the previous year. (Net levy is when you take the total levy and subtract the levy exempt items such as libraries and bridge aid then add personal property aid.) The result is a dollar amount which our levy is allowed to increase for the new year. This year Chippewa County is the 10th highest net new construction rate in the state due to economic growth.

Year	Net New Construction Percentage
2021 for 2022	1.98%
2022 for 2023	2.06%
2023 for 2024	2.47%
2024 for 2025	2.34%
2025 for 2026	1.92%

TAX LEVY

This is the combination of all department budgets line item 411100 "General Property Taxes". Remember this total will include some items which are not included in the net levy such as libraries, etc. The total proposed levy for the 2026 budget will be included with my final recommendation.

Year	County Levy	Increase from Previous Year	% Increase
2021 for 2022	$20,638,711	$685,569	3.44%
2022 for 2023	$20,941,066	$302,355	1.46%
2023 for 2024	$21,110,729	$169,663	.81%
2024 for 2025	$21,713,416	$602,687	2.85%
2025 for 2026	$22,393,725	$680,309	3.13%

711 N. Bridge Street, Room 106
Chippewa Falls, WI 54729
aalbarado@chippewacountywi.gov
Ph: (715)
Fx: (715)

EQUALIZED VALUE FROM WISCONSIN DEPARTMENT OF REVENUE (APPORTIONMENT REPORT-TID OUT)

We have received the final equalized valuation from Wisconsin Department of Revenue for this year's tax rate calculation. The equalized value is critical in the computation of the tax rate. The valuation has seen an increase of 10.39% from 2024. It is noteworthy that the valuation increase is attributable to approximately 8% in economic change and 2% of actual new construction.

Year	Equalized Valuation	Change	% Change
2021 for 2022	$6,662,368,300	$549,810,900	8.99%
2022 for 2023	$7,699,372,900	$1,037,004,600	15.57%
2023 for 2024	$8,806,721,900	$1,107,349,000	14.38%
2024 for 2025	$9,536,158,100	$729,436,200	8.28%
2025 for 2026	$10,526,745,400	$990,587,300	10.39%

STATE SHARED REVENUE

In 2024 a change in State Shared Revenue created a Supplemental payment in addition to the Legacy County Aid and Utility Aid. The new Supplemental Payment is expected to have a modest increase every year based on sales tax collections by the State. The projected increase for 2026 is 3.4%. Based on latest information received from the Wisconsin Counties Association and the Legislative Fiscal Bureau, we are anticipating an increase of 3.4% (or approximately $114,185) which is included in my preliminary tax levy, tax rate and maximum allowable levy above. However, the Wisconsin Department of Revenue will not release the final number until late September 2025.

Year	County Aid	Utility Aid	Supplemental County Aid	Total Shared Revenue	Increase	% Change
2022	$1,241,630	$1,332,150	-	$2,573,780		
2023	$1,241,629	$1,305,501	-	$2,547,130	($26,650.13)	-1%
2024	$1,241,564	$1,380,730	$741,795	$3,364,088	$816,958.48	32%
2025	$1,270,028	$1,329,494	$758,856	$3,358,378	($5,711)	-.1%
2026 (est.)	$1,313,209	$1,374,697	$784,657	$3,472,563	$114,185	3.4%

TAX RATE

The tax rate is a tax per dollar of assessed value of property. The rate is expressed in "mills". The tax rate is calculated by taking (tax Levy ÷ equalized value x 1,000 = tax rate). Our tax rate has been going down each year even though the levy amount has increased due to the increased equalized value.

Year	Tax Rate
2021 for 2022	$3.10
2022 for 2023	$2.72
2023 for 2024	$2.40
2024 for 2025	$2.28
2025 for 2026	$2.13 est.

711 N. Bridge Street, Room 106
Chippewa Falls, WI 54729
aalbarado@chippewacountywi.gov
Ph: (715)
Fx: (715)

MAXIMUM ALLOWABLE LEVY BY STATE (LEVY LIMITS)

All counties within Wisconsin have been under levy limits for several years. These levy limits only allow counties to increase their net levy from the previous year by net new construction and the annual debt payments. That is why I find it critical to keep the annual debt payments even or a slight increase from the previous year. If our annual debt payments decrease from the previous year, that would mean that we need to reduce levy and that will directly affect our employees.

Year	Allowable Levy	Allowable Tax Rate	Approved Levy	Approved Tax Rate	Amount Available to Levy Limit
2021 for 2022	$20,669,806	$3.10	$20,638,711	$3.10	$31,095
2022 for 2023	$21,022,125	$2.73	$20,941,066	$2.72	$81,059
2023 for 2024	$21,361,600	$2.43	$21,110,729	$2.40	$250,871
2024 for 2025	$21,996,660	$2.31	$21,713,416	$2.28	$283,244
2025 for 2026	$22,397,046	$2.13	TBD	TBD	$3,321

SUMMARY OF NEW/REMOVED POSITIONS

The table on the next page shows the new positions that the County Board approved for incorporation into the FY26 budgets. The table also includes 2025 mid-year requests that were approved by the County Board. All new positions listed below are currently included in the County Administrator FY26 Proposed Budget.

Summary of New/Eliminated Positions Recommended by the County Administrator

(The FY26 positions listed below have already been approved by the County Board and have been incorporated into the FY26 budget.)

Description	Department	Budget Process or Mid-Year	County Board Meeting	Comments
Administrative Assistant II (Part-Time)	DHS – ADRC	FY25 Mid-Year	Res 09-25 03/11/2025	Increased an LTE (975 hrs) to part-time (1500 hrs) to help the FT Elder Benefit Specialist until a second Elder Benefit Specialist can be created/hired. Funded with state & federal grants and levy.
Building Inspector – UDC (Full-Time)	Planning & Zoning	FY25 Mid-Year	Res. 26-25 07/08/2025	Create 2nd UDC inspector. Position will be paid for with fees and fees will increase starting in 2026.
CLTS Social Worker CWDA (Full-Time)	Human Services	FY26 Budget	Res. 28-25 08/12/2025	Created 1 position and will fill it at the beginning of 2026. Funded by Medicaid CLTS Waiver.
Elder Benefit Specialist (Part-Time)	Human Services	FY26 Budget	Res. 29-25 08/12/2025	Funded by an anticipated increase in the 2026 ADRC base grant. Position will be filled only if the 2026 ADRC base grant is increased by an amount sufficient to cover the estimated non-match cost of $31,457.
Legal Secretary (Part-Time)	District Attorney	FY26 Budget	Res. 30-25 08/12/2025	Created 1 part-time (1500 hr) position by utilizing the $50,000 of additional levy funding added to the department budget in 2025.

COUNTY ADMINISTRATOR PROPOSED BUDGET PRESENTED TO EXECUTIVE COMMITTEE

Just a reminder that my recommended budget will be presented at the October 7th Executive Committee meeting at 4:00 pm in Room 302. Anyone is welcome to attend.

NOVEMBER BUDGET HEARING AND REGULAR COUNTY BOARD MEETINGS

The budget hearing is scheduled for November 6th at 6:00 p.m. in Room 302. During this public hearing, community members will have the opportunity to share comments on the budget I have recommended to you. Once the hearing concludes, I will present the budget in the same form that was shared with the Executive Committee. At this meeting, you will be asked to make a motion to approve a balanced budget for 2026. Please keep in mind that if you wish to make changes to the recommended budget, it must remain balanced. In other words, any added expense must be matched with a corresponding revenue source. (A balanced budget means that total expenses equal total revenues, including the property tax levy.)
If you have any questions or concerns you may contact me at any time.

Sincerely,

Andy Albarado
County Administrator

711 N. Bridge Street, Room 106
Chippewa Falls, WI 54729
aalbarado@chippewacountywi.gov
Ph: (715)
Fx: (715)