AGENDA
1. Call Meeting to Order
2. Establish a Quorum ~ Roll Call
3. Adopt Agenda / Properly Noticed
4. Approve Minutes of April 13, 2021 Regular Administrative Committee Meeting
5. Correspondence
6. Public Comment
7. Old Business
8. New Business (Review / Action)
   ◆ County Board
      ♦ Self-Organized County Options
      ♦ Post COVID-19 Virtual Meetings (e.g., Teleconference, Videoconference, Internet-Based) Versus In-Person
      ♦ County Board Chair and/or Administrator Appointments to Committees, Commission, Boards – Rules/Procedure/Process
   ◆ County Administrator
      ♦ COVID-19
      ♦ Door County Government Operations
      ♦ Update and Review of Resolution 2021-31
      ♦ Transportation Program Update
   ◆ Corporation Counsel
      ♦ Amend Ch. 18, DCC-Record Retention Policy & Adopt WHS PRB General Records Schedule
      ♦ Resolution No. 2021-___ - HIPAA Policies and Procedures
   ◆ Human Resources
      ♦ HR Overview of Duties Refresher
      ♦ Request to Refill – Patrol Deputy and All Subsequent Vacancies
      ♦ Request to Refill – Comprehensive Community Services Case Manager and All Subsequent Vacancies
      ♦ Request to Refill – Library Custodian (part time)
      ♦ Personnel Transactions
9. Matters to be Placed on a Future Agenda or Referred to a Committee, Official, or Employee
10. Vouchers, Claims and Bills
11. Next Meeting Date(s)
12. Regular Meeting
   ♦ Tuesday, June 15, 2021 – 9:00 a.m.
13. Meeting Per Diem Code
14. Adjourn

Deviation from order shown may occur

In light of the declared state of emergency and to mitigate the impact of COVID-19 this meeting will be conducted by teleconference or video conference. Members of the public may join the meeting remotely or in-person.

To attend the meeting via computer:
Please click the link below to join:
https://us02web.zoom.us/j/83076003972?pwd=djkxcFlTOXAvVFFyU2ZvNUN0dlo2UT09
Webinar/Meeting ID: 830 7600 3972
Passcode: 277532
Or by Phone:
Dial: 1-312-626-6799

In compliance with the Americans with Disabilities Act, any person needing assistance to participate in this meeting, should contact the Office of the County Clerk at (920) 746 2200. Notification 72 hours prior to a meeting will enable the County to make reasonable arrangements to ensure accessibility to that meeting.
Call Meeting to Order
The Tuesday, April 13, 2021 Administrative Committee Meeting was called to order at 1:01 p.m. by Chairman David Lienau at the Government Center.

Establish a Quorum ~ Roll Call
Members present: David Lienau, Dan Austad, Ken Fisher, Susan Kohout, Nancy Robillard, Richard Virlee, and Joel Gunnlaugsson.

Others present: Supervisor David Enigl, Supervisor Bob Bultman, Administrator Ken Pabich, Assistant Corporation Counsel Karyn Behling, HR Director Kelly Hendee, Transportation Manager Pam Busch, TS Director Jason Rouer, and County Clerk Jill Lau.

Virtual Attendance: Staff and Public.

Adopt Agenda / Properly Noticed
Motion by Austad, seconded by Robillard to approve the agenda. Motion carried by voice vote.

Approve Minutes of March 16, 2021 Regular Administrative Committee Meeting
Motion by Virlee, seconded by Fisher to approve the minutes of the March 16, 2021 Administrative Committee Meeting. Motion carried by voice vote.

Correspondence
No correspondence was presented.

Public Comment
The following persons commented:
- Don Freix, Fish Creek

Old Business
No old business was presented.

New Business (Review / Action)
County Board
§59.11(1)(c), Wis. Stats. Organizational Meeting
Proposed Changes to Rules of Order
Each proposed rule change was reviewed.

Rule of Order 5. Agenda
Adds a point of clarification that the items must be germane to and fall in to the scope, procedures, and/or statutory authority of the county board. Most of the county board authority is granted through Chapter 59. Statutory references can be added.

Rule of Order 8. A. Regular Meeting Agenda 5. Correspondence
Adds clarification to correspondence: Correspondence included with the agenda packet is limited to matters that are germane to an agenda item and fall within the County’s statutory authority, responsibilities and roles. If pertains to an item on the agenda, must be in possession of the Administrator before noon on the sixth (6th) day prior to the scheduled board session to be included with the agenda packet. Discussion regarding receiving any correspondence after the 6th day and process to distribute to county board members.
Rule of Order 13 Consent to Speak
The proposed changes are clean-up and are to clarify existing rules. Consent to Speak / Participating in Debate
A. A member must be recognized by the Chairperson before speaking (e.g., introducing a resolution or ordinance, making a motion, or debating a question). B. No member may speak more than twice, or longer than three (3) minutes the first time and two (2) minutes the second time, on the same motion. C. No member is entitled to be called on to speak a second time in debate on the same motion until everyone who is seeking recognition has had their first opportunity to speak. D. Discussion must be limited to the merits of the specific motion that is being debated, not the general subject.

Rule of Order 15. Motions
Additional language to clarify. Motions to Amend: 1. Must be germane (i.e., closely related to or having bearing on the subject of the thing to be amended). This means that no new subject can be introduced under pretext of being an amendment. 2. That create a fiscal impact, which is defined as an unbudgeted expense per Sec. 65.90, Wis. Stats. a. The item shall be postponed to the next succeeding meeting or, b. If the item is timely, requires a 2/3 vote to pass at the same meeting if the fiscal impact can be properly determined, and c. The Finance Director or Administrator is to determine whether a proposed amendment has a fiscal impact and, and if so, the estimated amount. 3. If results in substantive change, consideration of the matter may be postponed (until later in the same meeting or the next succeeding meeting). 4. If adopted, the Administrator or Finance Director will report back at the next succeeding meeting as to any unplanned allocation or consumption of internal (human and other) resources that results from the amendment.

Rule of Order 27. Public Addressing Board, B. Public Comment
The proposed change narrows comments down to what the Board actually has control of and are within their roles, responsibilities and statutory authority.

Motion by Kohout, seconded by Gunnlaugsson to approve the changes as presented and move on to County Board. Motion carried by voice vote.

Legislative Committee Duties
Suggested changes to the duties were included in the meeting packet and were reviewed.

Motion by Virlee, seconded by Robillard to approve the draft duties as presented and move on to County Board. Motion carried by voice vote.

Agenda Order
Reviewed.

Self-Organized County Options
Reviewed. Any proposed changes allowed by being self-organized should be brought forward soon as to have time to discuss and possibly act on.

Post COVID-19 Virtual Meetings (e.g., Teleconference, Videoconference, Internet-Based) Versus In-Person
Discussion of continuing virtual attendance at both County Board and Committee meetings. Once the Emergency DOJ Rule ends the Board will need to have a process in place related to virtual attendance. Discussion followed. This agenda item will be brought back next month.

County Administrator
COVID-19
Expenses related to the clinics continue. A financial update will be provided in the near future. Door County leads the state in vaccine rollout. The County has hired 12 nurses to assist with the clinics on a limited basis. Katie VanLaanen is organizing the clinics and supervising the nurses. Administrator Pabich asked to allow a temporary increase of $1.25/hr for Katie during the organizing phase.

Motion by Austad, seconded by Robillard to approve a temporary $1.25/hr increase for Katie VanLaanen. Motion carried by voice vote.

Door County Government Operations
Administrator Pabich noted the buildings are open. In terms of operations, county personnel will continue in this phase through at least next month with at least 50% of their time working in the building. Public is encouraged to
make appointments with departments if they need in person services.

2020 Carryover – General Finance Special Projects Wage Plan
Administrator Pabich is requesting a $10,412 carryover from 2020 Special Project line to 2021 for use in data collection related to our negotiations with the represented units.

Motion by Robillard, seconded by Kohout to approve the request for the carryover. Motion carried by voice vote.

Transportation Program Update
Transportation Director Pam Busch provided a written report in the meeting packet which was reviewed. Volunteer time was reviewed; what is the easiest way for a committee member to report volunteer time. Volunteer time includes time spent reading the transportation update.

Acceptance of Wis DOA – DEHCR 2021 CDBG Award for CL-HSG Project
Administrator Pabich reported the County was awarded $1.447M for the Community Development Block Grant. A resolution is needed to accept the funding and the adoption of a written procurement purchasing procedures policy is required.

Motion by Fisher, seconded by Robillard to accept the DEHCR 2021 CDBG award. Motion carried by voice vote.

Adoption of Written Procurement / Purchasing Procedures – Wis DOA – DEHCR 2021 CDBG Award for CL-HSG Project
Motion by Fisher, seconded by Robillard to adopt the procurement policy as drafted. Motion carried by voice vote.

Corporation Counsel
Thomson Reuters Westlaw Subscription Renewal
Assistant CC Behling reviewed information included in the meeting packet and explained this is a subscription renewal for a legal update service used in the department.

“Navis et. al. -vs- Door County BOA, et. al.” Wis Ct of App’s Decision
Information included in the meeting packet was reviewed. The court upheld the decision of the BOA.

Human Resources
2020 Annual Budget Report
The report was included in the meeting packet and was reviewed.

Request to Refill – Administrative Assistant 1 – Register in Probate
Motion by Fisher, seconded by Kohout to approve the request to refill the Administrative Assistant 1 in Register of Probate. Motion carried by voice vote.

Request to Refill – Captain – Emergency Services
The request was reviewed and approved by the Public Safety Committee.

Motion by Gunnlaugsson, seconded by Kohout to approve the request to refill the Captain position in Emergency Services and all subsequent positions. EMS Director Aaron LeClair reviewed the need for the Captain positions; discussion followed. Motion carried by voice vote with Supervisor Virlee voting no.

Request to Refill – Network Technician – Technology Services
Motion by Fisher, seconded by Virlee to approve the request to refill the Network Technician – Technology Services. Motion carried by voice vote.

Request to Refill – Security Sergeant – Sheriff’s Office
Motion by Fisher, seconded by Gunnlaugsson to approve the request to refill the Security Sergeant in the Sheriff’s Office. Motion carried by voice vote.

Motion by Fisher, seconded by Gunnlaugsson to fill all subsequent vacancies. Motion carried by voice vote.
Personnel Transactions
Reviewed.

Matters to be Placed on a Future Agenda or Referred to a Committee, Official, or Employee
Nothing as of this meeting.

Vouchers, Claims and Bills
Reviewed.

Next Meeting Date(s)
Regular Meeting
  • Tuesday, May 18, 2021 – 9:00 a.m.

Meeting Per Diem Code
413.

Adjourn
Motion by Fisher, seconded by Kohout to adjourn. Time 2:35 p.m. Motion carried by voice vote.

Respectfully submitted by Jill M. Lau, County Clerk
TO: Administrative Committee

FROM: Ken Pabich, County Administrator

DATE: May 18, 2021

RE: Resolution 2021-31 Door County Vision of Diversity, Equity and Inclusion (DEI)

Background
The adopted Resolution 2021-31 states that the Administrator shall work with the Administrative Committee to develop a plan moving DEI forward. In addition, there have been questions on the amended resolution and how it relates to the newly adopted County Board rules. In short, the new rules require the Administrator or Finance Director to address the following for an amendment:

1. Does the amendment create an unplanned budgeted fiscal impact, which triggers Sec. 65.90, Wis. Stats.?
2. Does the amendment create any significant unplanned allocation or consumption of internal (human and other) resources?

Analysis:
In short, the resolution as amended does not create an unbudgeted expense per Sec. 65.90, Wis. Stats. and it does not impact our internal resources if the following is considered reasonable by the Administrative Committee:

1. External DEI Plan Approach:
The external DEI Plan is defined as the community working together to advance making Door County more diverse, equitable and inclusionary. For this initiative, the County is a “passenger on the bus” but it is not the “driver” in pushing the topic forward. With this approach, I have reached out to various community leaders to help develop a plan in how this may be accomplished.

Fiscal Impact: To be determined and provided for as part of the annual (2022 and beyond) Sec. 65.90, Wis. Stats. budget process.

Internal Resource Impact: I would assume that staff or maybe supervisor(s) may be a part of the process; however, I would not consider this participation to be significant on the organization.

Feedback / Tracking: In this case, we are a participant in the process. As this moves forward, updates can be provided to the Administrative Committee and County Board as necessary.
2. **Internal DEI Plan Approach:**
The internal DEI Plan is defined as our organizational approach to advance making Door County more diverse, equitable and inclusionary as an organization and in the services that we provide. For this initiative, the County is “the driver” in pushing the topic forward.

For this approach, I am working with a team of Department Heads to define our overall approach and while it is not fully vetted this would be the general plan:

**Phase I:** Seek out and develop resources for training on DEI. Start with common definitions/vocabulary to provide a basic framework so supervisors and DH’s can assess current County operations. We would also look at ways to provide educational materials to all employees. (Timeframe: Now – October).

**Phase II:** Complete an internal assessment of where County operations are currently. This assessment would then be used to define what is needed for the next phase and potential budgetary items. (Timeframe: October - December).

**Phase III:** External assessment of what clients think of the County operations currently. (Timeframe: December - February).

**Phase IV:** Develop a plan of action with measurable goals and objectives. (Timeframe: February – May)

**Phase V:** Implementation and monitoring (Timeframe: On-going)

**Fiscal Impact:** To be determined and provided for as part of the annual (2022 and beyond) Sec. 65.90, Wis. Stats. budget process; however most of it can be included into the 2022 budget process.

**Internal Resource Impact:** It would require Administration and Department Heads to devote time to complete the phases outlined. If the timeframe is acceptable, it seems reasonable to work these phases into the project workflow of the departments.

**Feedback / Tracking:** As this moves forward, updates can be provided to the Administrative Committee and County Board as necessary.

**NOTE:** While the internal workplan may seem to long in duration, there is a significant amount of work that needs to be complete to properly address the items related to DEI.

**Recommendations:**
If the DEI approach defined above is acceptable then:

1. There is no unplanned fiscal impact which triggers Sec. 65.90, Wis. Stats, and
2. While there definitely is an added workload, this workload is manageable and it does not create a significant impact on our department’s operations.
Ridership:
Door County Connect-Door 2 Door Rides provided 8,267 rides last quarter. This is a decrease from last year where 9,818 rides were provided. April numbers were not available at the time of this report.

Door County Connect (former ADRC service) provided 601 trips last quarter. This is a decrease from last year where 1,195 trips were provided in the first quarter. 197 trips were provided in April.

Connector Link:
The deviated fixed route began May 12th. This service will operate every Wednesday from 8 a.m. to 4 p.m. Stops are at three businesses/bus stop sponsors and five residential areas. There is no cost to riders.

We are grateful for the volunteers who will be operating this service.

Schedule as of 5/13/21:

<table>
<thead>
<tr>
<th>Location</th>
<th>Morning Stops by Time</th>
<th>Afternoon Stops by Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADRC</td>
<td>8:15 AM</td>
<td>10:06 AM</td>
</tr>
<tr>
<td></td>
<td>11:52 AM</td>
<td>12:35 PM</td>
</tr>
<tr>
<td>Bay Hill Apartments</td>
<td>8:25 AM</td>
<td>10:19 AM</td>
</tr>
<tr>
<td></td>
<td>11:17 AM</td>
<td>12:48 PM</td>
</tr>
<tr>
<td>Big Hill Apartments</td>
<td>8:32 AM</td>
<td>10:27 AM</td>
</tr>
<tr>
<td></td>
<td>11:23 AM</td>
<td>12:56 PM</td>
</tr>
<tr>
<td>Bay View Terrace/Neenah Ave Apts</td>
<td>9:18 AM</td>
<td>11:38 AM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1:20 PM</td>
</tr>
<tr>
<td>Door County Medical Center/Clinic Entrance</td>
<td>8:47 AM</td>
<td>9:32 AM</td>
</tr>
<tr>
<td></td>
<td>10:43 AM</td>
<td>1:35 PM</td>
</tr>
<tr>
<td>Econo Foods</td>
<td>9:04 AM</td>
<td>9:51 AM</td>
</tr>
<tr>
<td></td>
<td>11:02 AM</td>
<td>1:58 PM</td>
</tr>
<tr>
<td>Orchard Valley Apts</td>
<td>8:18 AM</td>
<td>9:58 AM</td>
</tr>
<tr>
<td></td>
<td>11:09 AM</td>
<td>12:38 PM</td>
</tr>
<tr>
<td>Pick 'n Save</td>
<td>8:57 AM</td>
<td>9:42 AM</td>
</tr>
<tr>
<td></td>
<td>10:53 AM</td>
<td>1:43 PM</td>
</tr>
<tr>
<td>Thunderhill Estates (Delaware Drive)</td>
<td>8:39 AM</td>
<td>10:35 AM</td>
</tr>
</tbody>
</table>

Above times may change. Bus stop signs will have updated arrival & departure times.
Service Every Wednesday
8:15am–4:00pm
Starting 5/12/21

The Connector Link

Door County Connect (formerly called ADRC Bus/Van Service) is part of the public transit system in Door County. Recently, we expanded services to offer an even more affordable travel option for our community! The Connector Link is a deviated route, that connects multi-family residential areas to businesses that sponsor a bus stop. There is no cost to ride the Connector Link.

Please Note: Door County Connects’ regular demand service will continue to operate on Wednesdays without any change in service or cost.

Schedule as of 5/13/21:

<table>
<thead>
<tr>
<th>Location</th>
<th>Morning Stops by Time</th>
<th>Afternoon Stops by Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADRC</td>
<td>8:15 AM</td>
<td>10:06 AM 11:52 AM</td>
</tr>
<tr>
<td></td>
<td>12:35 PM 2:21 PM 3:59 PM</td>
<td></td>
</tr>
<tr>
<td>Bay Hill Apartments</td>
<td>8:25 AM</td>
<td>10:19 AM 11:17 AM</td>
</tr>
<tr>
<td></td>
<td>12:48 PM 2:29 PM 3:24 PM</td>
<td></td>
</tr>
<tr>
<td>Big Hill Apartments</td>
<td>8:32 AM</td>
<td>10:27 AM 11:23 AM</td>
</tr>
<tr>
<td></td>
<td>12:56 PM 2:37 PM 3:31 PM</td>
<td></td>
</tr>
<tr>
<td>Bay View Terrace/Neenah Ave Apts</td>
<td>9:18 AM</td>
<td>11:38 AM 12:00 AM</td>
</tr>
<tr>
<td></td>
<td>1:20 PM 3:45 PM</td>
<td></td>
</tr>
<tr>
<td>Door County Medical Center/Clinic Entrance</td>
<td>8:47 AM</td>
<td>9:32 AM 10:43 AM</td>
</tr>
<tr>
<td></td>
<td>1:35 PM 2:53 PM</td>
<td></td>
</tr>
<tr>
<td>Econo Foods</td>
<td>9:04 AM</td>
<td>9:51 AM 11:02 AM</td>
</tr>
<tr>
<td></td>
<td>1:58 PM 3:09 PM</td>
<td></td>
</tr>
<tr>
<td>Orchard Valley Apts</td>
<td>8:18 AM</td>
<td>9:58 AM 11:09 AM</td>
</tr>
<tr>
<td></td>
<td>12:38 PM 2:06 PM 3:17 PM</td>
<td></td>
</tr>
<tr>
<td>Pick ’n Save</td>
<td>8:57 AM</td>
<td>9:42 AM 10:53 AM</td>
</tr>
<tr>
<td></td>
<td>1:43 PM 3:01 PM</td>
<td></td>
</tr>
<tr>
<td>Thunderhill Estates (Delaware Drive)</td>
<td>8:39 AM</td>
<td>10:35 AM 1:05 PM</td>
</tr>
<tr>
<td></td>
<td>2:45 PM</td>
<td></td>
</tr>
</tbody>
</table>

*Above times may change based on service needs. Bus stop signs will have updated arrival & departure times.

The Connector Link is offered with the help of volunteers. Please call Pam Busch at 920-746-5982 to learn more.

Get on Board. Get Connected.

Find out more at www.doorcountyconnect.com.

NO cost to ride the Connector Link. Limit of 4 packages.

Unable to get to a bus stop or have more than 4 packages? If so, call 920-746-6944 to learn about other options.
Introduction to General Records Schedules

Revised 11/2017

For use by

All units of Wisconsin Government at the State, County, and Municipal level
INTRODUCTION

Records are a basic tool of transacting business on behalf of all units of Wisconsin Government at the State, County, and Municipal level. They are also the foundation for government accountability.

Records management is regulated by Wisconsin state law, and accordingly, General Records Schedules (GRSs) provide legal authorization to dispose of records common to a business function on a regularly scheduled basis. General Records Schedules are a mechanism for consistent retention and disposition of similar types of records across all government units and provide assurance of accountability to the public. GRSs also contain guidelines for complying with legal, fiscal, and archival requirements for records retention and facilitate cost-effective management of records commonly found in all government units.

The records retention obligations of state agencies are governed by Wis. Stat. § 16.61 and apply to “public records” as defined in Wis. Stat. § 16.61(2)(b). These materials are referred to as “records” in this document for ease of reference. Records that are unique to a specific government unit require the creation of a separate Records Disposition Authorization (RDA) that must be submitted by the entity, and approved by, the Public Records Board (PRB).

I. PURPOSE

The purpose of a General Record Schedule is to:

• Provide agencies with uniform guidelines for the retention and disposition of records common to a business function;

• Ensure that agencies retain records as long as needed in order to complete the transaction of business on behalf of the State of Wisconsin, and to meet legal, audit, archival, and other State of Wisconsin and federal requirements;

• Provide agencies with legal authorization to dispose of records eligible for disposition on a regularly scheduled basis after the minimum retention periods are met. Records may not be disposed of in a shorter period of time; and

• Promote the cost-effective management of records.

II. WHO MAY USE GENERAL RECORDS SCHEDULES

When the PRB approves a General Records Schedule, its use is mandatory for all state agencies except the UW System Administration (UWSA) and its institutions. State agencies may request, and gain approval from, the PRB to either: adopt some, but not all, of the schedules contained within the document, or adopt an independent set of records schedules. Wisconsin counties, municipalities, other local units of government and the UWSA are encouraged to use the applicable GRS. To do so, each entity must take affirmative action to adopt a GRS by completing the Notification of General Schedules Adoption (PRB-002) form. Units of Wisconsin Government are then expected to supersede previously approved, unique, RDAs now covered by an approved GRS. For additional information on opting in to and out of a GRS see the General Records Schedule Policy.

III. RECORDS RESPONSIBILITIES

Most agencies do not create or receive all of the records listed within a General Records Schedule. Thus it is important to note that GRSs do not require records to be created by agencies. Rather, an approved GRS provides guidance for records that are actually created or received by government agencies in their course of work.

Under Wisconsin law, each government unit is responsible for properly managing its records with approval from the Public Records Board. Proper records management can become complex, especially...
when: the same records are held by more than one department within a government unit, or multiple units possess the same records. Accordingly, GRSs provide guidance for:

a) Records management among the departments of a single government unit, all of which have custody of the same or similar records; and

b) Records management among different government units, all of which have custody of the same or similar records. This primarily occurs between an operating state agency and agencies with statewide oversight such as the Department of Administration (DOA). An example would be the agency biennial budget request submittal to the State Budget Office in DOA. This is a record for both the state agency that develops and submits the biennial budget request as well as the State Budget Office in DOA which receives the agency biennial budget request as a starting point in developing the Governor’s Biennial Budget. Both DOA and the state agency have official public records in this example.

IV. RECORD SERIES TITLES AND CATEGORIES

Each GRS contains a table listing the series title and categories for that particular record series. Below is an example of the format used in GRSs and an explanation of each column.

<table>
<thead>
<tr>
<th>RDA Number</th>
<th>Record Series Title</th>
<th>Series Description</th>
<th>PII</th>
<th>Confidential</th>
<th>Minimum Retention and Disposition</th>
<th>Event Description</th>
<th>Examples/Notes</th>
<th>Previous RDA Number (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RDA Number:** A unique identifying number for each record series.

**Record Series Title:** A descriptive title that defines the record series.

**Series Description:** A brief description of the record series.

**PII:** Indicates whether or not records in the record series may contain personally identifiable information as defined in Wis. Stat. § 19.62(5). See section V. a) of this document for more information.

**Confidential:** Indicates whether or not records in the record series may contain confidential information. If yes, the GRS requires a rationale for the confidential designation such as a statute, administrative rule, or other legal authority. See section V. b) of this document for more information.

**Minimum Retention and Disposition:** Indicates the minimum time period a record series must be maintained expressed in years, months or days and the designation of whether or not the record series has been identified as having historical value warranting preservation at the State Archives or University of Wisconsin Archives. This section also notes if a record is to be destroyed confidentially. Records must be retained for the minimum retention time approved in the GRS and cannot be disposed of in a shorter amount of time.

**Event Description:** The description of what initiates the start of the retention clock. For example, the retention of some record series may be the close of the state fiscal year (June 30, xxxx) and for others the close of the calendar year (December 31, xxxx). Other record series have events based upon something occurring, such as the date a person leaves state employment or the date a loan is repaid.
Example/Notes: Provides additional guidance and/or provides applicable examples to assist in interpreting the relevancy of the record series.

Previous RDA Number (if applicable): Identifies prior RDA numbers for record series that have been superseded or closed by the current GRS.

V. CONFIDENTIALITY AND PERSONALLY IDENTIFIABLE INFORMATION (PII) OF RECORD SERIES CONTAINED WITHIN GENERAL RECORDS SCHEDULES

a) Personally Identifiable Information (PII)

Wisconsin law defines Personally Identifiable Information (PII) as information that can be associated with a particular individual through one or more identifiers or other information or circumstances (Wis. Stat. § 19.62(5)), and requires authorities to identify certain record series within a GRS that contain PII.

Despite the broad definition, Wis. Stat. § 16.61(3)(u) requires that record series within a schedule containing the following types of PII need not be identified as such: a) mailing lists; b) the results of certain computer matching programs; c) telephone or e-mail directories; d) record series pertaining exclusively to agency employees; and e) those relating to state agency procurement or budgeting.

Some, but not all, records in a record series may contain PII. The PII column should be marked “yes” if some records in the series may contain PII. As to those record series identified as containing PII, the schedule further indicates whether the PII is incidental to the primary purpose for which the record series is created. If in doubt as to whether a specific record series contains PII, check first with your designated records officer. If necessary check with legal counsel.

Some PII, but not all, is confidential. In addition, some records in a series, but not all records in the same series, might contain confidential information. Finally, records not containing PII may be required by law to be kept confidential. The designation of a particular record series as “confidential” relates primarily to the schedule’s function in regulating the retention and disposition, including destruction, of the record series. See the next section for more information. In contrast, public access to records is determined by the Public Records Law and not simply by the designation of confidentiality in a record schedule.

b) Confidentiality of Records

Some records series may contain confidential or restricted access records. The GRS will identify any record series containing information required by law to be kept confidential or specifically required to be protected from public access, identifying the state or federal statute, administrative rule, or other legal authority that so requires. Some, but not all, records in a records series may contain confidential information. The confidential column should be marked “yes” if some records in the series may contain confidential information. Even when specific confidentiality statutes do not apply, application of substantive common law principles through the balancing test considerations under Wis. Stat. § 19.35(1)(a) may affect disclosure of the record under the public records law. For example, some of those considerations include information relating to mental and physical health, victim information, privacy, and records protected by attorney client privilege or attorney work product. In addition, when an individual or an individual’s representative makes an open records request for records containing personally identifiable information about that individual, there is no balancing test but the disclosure exceptions under Wis. Stat. § 19.35(1)(am) must be considered. The Wis. Stat. § 19.35(1)(am) exceptions include endangering an individual’s life or safety; endangering the security of a prison, including the security of the population or staff; identifying a confidential informant; and records collected or maintained in
connection with complaints, investigations, or other circumstances that may lead to various administrative or court proceedings. Consultation with agency legal counsel is recommended when responding to an open records request.

VI. RECORDS FORMAT

Records retention guidelines apply regardless of record format. Records covered by any GRS may be retained in electronic, paper, or other formats. The schedule applies to all records born digital (including those created or transmitted via e-mail), data contained in database systems, tapes/cartridges and other types of electronic records and information systems maintained by agencies. To safeguard the information contained in records maintained exclusively in electronic format, agencies must meet the standards and requirements for the management of electronic records outlined in Wis. Admin. Code ch. Admin 12.

VII. RETAINING RECORDS

General Record Schedules provide the minimum retention time a government unit must retain records. Records may not be destroyed earlier under any circumstances. Also, if a record series is identified as having historical value, those records must be transferred to the appropriate designated archival repository for preservation instead of being destroyed by the government unit.

After the required minimum retention time period has been met, records should be destroyed or transferred unless any of the following conditions apply:

a) Records are required for financial or performance audits either currently underway or known to be planned.
b) Records are subject to a “legal hold” because they may be relevant to an existing, pending, or anticipated legal proceeding.
c) A related open records request has been received and not completed, or statutorily required time periods have expired.

VIII. REPOSITORIES

a) Archival

For records series that have been appraised as having long-term value, the disposition will indicate “transfer to an archival repository.” An archival repository is responsible for processing the records, making them available to researchers, and providing for their safe-keeping and preservation. An official archival repository is one that has been reviewed and designated as such by the Wisconsin Public Records Board according to Wis. Stat. § 16.61(13)(b). In general, transferring to an archival repository means transferring records to either the State Archives in the Wisconsin Historical Society (for state agencies and local units of government) or the applicable University of Wisconsin Archives (for University of Wisconsin records). The State Archives captures the public-facing web content of government units on a regular basis. Preserved websites are available through the Internet Archive.

b) Wisconsin Document Depository Program

Under Wis. Stat. §§ 35.81-35.84 state agencies are required to participate in the Wisconsin Document Depository Program. The Wisconsin Document Depository Program collects and distributes state documents in print and electronic formats to Wisconsin libraries; preserves and makes available a record of major state government programs; and assures the availability of state documents for use by the public throughout Wisconsin now and in the future. Print documents are distributed to designated depository libraries throughout the state. Electronic documents are digitally archived and made accessible through the Wisconsin Digital Archives. For more information about the program visit the website or email statedocuments@dpi.wi.gov.
Many state publications are now born-digital, which is, published only on the Web or only maintained in an electronic format. Electronic publications are collected and preserved as part of the Wisconsin Document Depository Program; URLs to state publications published electronically on Wisconsin State Agency websites should be emailed directly to statedocuments@dpi.wi.gov as a way for state agencies to fulfill the statutory obligation to participate in the Wisconsin Document Depository Program.

IX. FOR ADDITIONAL INFORMATION AND ASSISTANCE

For help interpreting or applying this schedule to your records, or help organizing your records, contact your organization’s designated records officer.

Agency Counsel: Agency counsel can assist with legal issues related to records retention, such as identification of confidentiality requirements.

Records Officer: Each state agency has a designated records officer who serves as liaison to the Public Records Board. The records officer is responsible for agency-wide records management planning, program development, and assistance.

Additional information and assistance with records management concerns is also available from the following sources:

DOA Records Management Section:
The DOA Records Management Section, via the State Records Center, provides additional information on records management.

Public Records Board:
The Board’s Executive Secretary can offer technical assistance and training to assist agencies with records management, including records scheduling and interpretation of schedules.

Wisconsin Historical Society:
The Wisconsin Historical Society (WHS) assists agencies with records management, particularly in identifying the small percentage of records that have historical value.

University of Wisconsin Institution Archives:
University of Wisconsin Institutions has delegated authority to operate archives for historical institutional records. Often, the University of Wisconsin archives also function as the focus for records management related activities on the campus.
General Records Schedule Policy

Upon Public Records Board (PRB) approval of a General Records Schedule (GRS), the implementation of said schedules by Wisconsin state agencies is mandatory and immediate. Implementation of a PRB-commissioned GRS by the UW System Administration, all UW campuses, all Wisconsin counties, municipalities or other local units of government is optional but recommended. This policy is in accordance with the authority outlined under Wis. Stats. § 16.61.

Policy Statement

General Record Schedules are a mechanism for systematic retention and disposition of similar types of records across all government units. GRSs eliminate the need for state agencies to develop and seek approval of their own records retention disposition authorizations (RDAs). They lend consistency to recordkeeping across all government units and provide assurance of accountability to the public. The PRB supports the development of, and has approved, GRSs in several functional areas. This policy statement mandates usage and implementation of these schedules, as well as outlines a process and requirements that state agencies must use to opt out of any or all of them, in whole or in part. See page 3 for implementation guidance and frequently asked questions. For additional information on use of the GRS see the Introduction to General Records Schedules.

All state agencies are bound by this policy. State agencies may choose to opt out of a GRS, in whole or in part; however, to opt out in whole or in part, an agency must develop corresponding RDAs of their own within 12 months from the date of the GRS approval, citing justification for the unique requirement. During that time, and until their replacement, the agency will be bound by retention schedules which have been approved by the PRB in the General Records Schedule.

UW System Administration, all UW campuses, all Wisconsin counties, municipalities or other local units of government may:

**Opt In:** The UW System Administration, all UW campuses, all Wisconsin counties, municipalities or other local units of government may opt in, using the Notification of General Schedule Adoption form (PRB-002), and agree to use the recommendations noted in the GRS for its records. (*State agencies do not have this option because any GRS is mandatory and immediate on approval*).

**Opt In with Revisions:** The UW System Administration, all UW campuses, all Wisconsin counties, municipalities or other local units of government may opt in with revisions using the Notification of General Schedule Adoption form (PRB-002). They agree to use some of the recommendations of the GRS and also submit a list of records series they will be opting in to or out of. They must develop and submit to the PRB corresponding records series of their own within 12 months from the date of GRS approval for any record series they opt out of. It is recognized that local units may in some areas have the need to retain items for a longer period of time than that recommended by the GRS. This is an internal business decision and can be done without any action. (*State agencies do not have this option because any GRS is mandatory and immediate on approval*).

State agencies, UW System Administration, all UW campuses, all Wisconsin counties, municipalities or other local units of government may:

**Opt Out:** State agencies may opt out of a GRS in whole or in part, using the Notification of General Schedule Adoption form (PRB-002). The agency must develop, and submit to the PRB, within 12 months, RDA(s) for
the records covered by the GRS which they chose to opt out of citing justification for the unique requirement. Until they receive PRB approval for those RDAs, they will be bound by the GRS.

State agencies should be aware that current law (Wis. Stat. § 16.61) requires authorization of the PRB to destroy any state agency records. Therefore, if a state agency chooses to opt out of any existing GRS, they may not dispose of any records until the RDAs prepared by the state agency have been approved by the Public Records Board and the retention period reached.

Wisconsin counties, municipalities and other local units of government should be aware of how current law (Wis. Stat. § 19.21(4)(b) & (5)(c) respectively) addresses record retention and disposition, as well as PRB authorization.
Implementing General Records Schedules

Upon PRB approval, agencies will use an identified GRS for any applicable records in its custody. This means that following approval, records should continue to be disposed on a regular basis, provided that the minimum retention time identified in the GRS has been met. Records must be retained for the minimum retention time approved in the GRS and cannot be disposed of in a shorter amount of time. If a GRS identifies a record series with a disposition of transfer to an archival repository, those records must be offered to the archival repository rather than being destroyed. Destruction or transfer of records is contingent on record disposition restrictions contained in Wis. Stat. § 19.35 (Open Records Law). No records may be destroyed or transferred if litigation or audit involving the records has commenced.

State agencies may discontinue the use of all, or portions of, any GRS, but the agency records officer must first notify the PRB of the discontinuance, by following the steps noted in the policy above. When an agency discontinues use of a GRS, the records controlled by the applicable record series may no longer be destroyed or transferred until separate RDAs are prepared by the agency and approved by the PRB. Until that time, the agency must continue to abide by the retention and disposition in the existing GRS.

General Records Schedule (GRS) -- Frequently Asked Questions

1. **What happens to pre-existing General Records Schedules when an amended or renewed GRS is approved?**

   The pre-existing GRS is superseded by the new GRS immediately upon approval.

2. **What happens when a General Records Schedule (GRS) automatically goes into effect?**

   Upon Public Records Board (PRB) approval of a General Records Schedule (GRS), the implementation of said schedules by Wisconsin state agencies is mandatory and immediate.

3. **What happens to any pre-existing agency Records Disposition Authorizations (RDAs) on topics covered by a General Records Schedule (GRS)?**

   a. Pre-existing agency RDAs with a longer retention period stand until their sunset date is reached.

      i. The agency Records Officer should submit the appropriate form to formally supersede the pre-existing RDA before the sunset date is reached.

   b. Pre-existing agency RDAs with a shorter retention period must be acted on within 12 months of the GRS approval date. Until that time, the agency must abide by the GRS. Appropriate action includes: superseding or amending.

      i. The agency Records Officer should submit the appropriate form to supersede or amend the pre-existing RDA.

   c. Any pre-existing RDAs with a shorter retention period which the agency does not act on within 12 months, will become obsolete and

      i. The longer GRS mandated retention time must be followed and

Revised November 2017
ii. The agency Records Officer must submit the appropriate form to formally close the pre-existing RDA.

4. **Why would an agency business unit choose to submit their own RDA for records covered by a GRS RDA?**

   a. Unique retention requirements for a set of specific business unit records. Requested retention period cannot be shorter than the approved GRS retention.

   b. Unique disposition requirements for a set of specific business unit records which is different than the approved GRS.

   Note: A state agency cannot dispose of records covered by the GRS until the business unit RDA is approved by the PRB.

5. **What happens when the entire agency opts out of a GRS in whole or in part?**

   State agencies may opt out of a GRS in whole or in part, using the Notification of General Schedule Adoption form (PRB-002). The agency must develop and submit to the PRB, within 12-months, RDA(s) for the records covered by the GRS which they chose to opt out of citing justification for the unique requirement. Until they receive PRB approval for those RDAs, they will be bound by the GRS. Appropriate justification includes: statute, code, or other legal authority.
Notification of General Records Schedule Adoption

Schedule Title: ___________________________________________________________ Date: _________________

Instructions:

Complete and send the original and 2 copies to: State Archivist, Wisconsin Historical Society (WHS), 816 State St., Madison, WI 53706.

- Do not opt out of a record series because your agency does not create or use these types of records. Signing the form does not obligate an agency to create records. It only requires that records be retained in accordance with the retention time periods and dispositions if such records exist. See the Introduction to General Records Schedules for more information.

- Attach a brief narrative explaining your rationale for opting out of each record series. When a separate schedule is prepared, identify that the record series is in lieu of the general schedule and cross reference the specific series.

**NOTE: Destruction or transfer of records is not permitted until this form is signed by the WHS and the Public Records Board.**

Wisconsin Government Agency: ____________________________________________________________

Address: __________________________________________________________________________

This is to notify the Wisconsin Historical Society and the Public Records Board that the agency named above has reviewed the general records schedule and taken the following action (check appropriate box):

☐ Opt In: We adopt the entire schedule. (Available for University of Wisconsin [UW] System and Local Units of Government)

☐ Opt In With Revisions: We opt (out of), (in to), (circle one) the following record series. (Available for UW System and Local Units of Government) List the specific retention schedule numbers and titles:

________________________________________________________________________________________

________________________________________________________________________________________

☐ Opt Out: We opt out of the general records schedule (in whole), (in part), (circle one). (Available for State Agencies) *(All applicable records disposition must cease until separate retention schedules are developed and approved by the Public Records Board.)* List the specific retention schedule numbers and titles:

________________________________________________________________________________________

________________________________________________________________________________________

Agency Head/Deputy Signature __________________________ Date Signed _________________

Agency Records Officer Signature __________________________ Date Signed _________________

The Public Records Board and Wisconsin Historical Society acknowledge your Notification of Adoption. You are hereby authorized to retain, transfer, and dispose of records as indicated on the schedule.

State Archivist Signature __________________________ Date Signed _________________

PRB Executive Secretary Signature __________________________ Date Signed _________________
**Resolution No. 2021-___**

**HIPAA Policies and Procedures**

TO THE DOOR COUNTY BOARD OF SUPERVISORS:

WHEREAS, The importance of compliance with the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated by the United States Department of Health and Human Services thereunder (“HIPAA”) is hereby reaffirmed; and

WHEREAS, The proposed HIPAA Policies and Procedures, attached hereto as Addendum A and incorporated by reference herein as if fully set forth, are reasonable, appropriate for Door County’s size, functions and capabilities, and demonstrate a commitment on the part of Door County (i.e., its elected officials, appointed officials and employees) to be aware of and conduct itself (themselves) in accordance with privacy and security requirements and standards set forth in HIPAA;

WHEREAS, These HIPAA Policies and Procedures are intended to supplement, not supplant, existing policies and procedures (e.g., the Door County Department of Health & Human Services’ Confidentiality Policies); and

WHEREAS, These HIPAA Policies and Procedures are to be reviewed and amended from time to time as deemed necessary by and at the discretion of Door County.

NOW, THEREFORE, BE IT RESOLVED, By the Door County Board of Supervisors (“County Board”) that the HIPAA Policies and Procedures, attached hereto as Addendum A and incorporated by reference herein, are hereby approved and adopted.

BE IT FURTHER RESOLVED, That County Board hereby designates: the Corporation Counsel and/or their designee(s) as Privacy Official; Technology Services Department Director as Security Official; and the Human Resources Director as contact person or office responsible for receiving complaints about any failure to comply with HIPAA policies and procedures. The Privacy Official, Security Official and contact person each report to the County Administrator.

BE IT FURTHER RESOLVED, That the administrative functions of Door County’s group health plan(s) are performed by TPA’s. TPA’s perform all of each health plan’s covered functions and assume the obligations to comply with HIPAA policies and procedures.

**SUBMITTED BY:**
Administrative Committee

<table>
<thead>
<tr>
<th>David Lienau, Chairman</th>
<th>Joel Gunnlaugsson</th>
</tr>
</thead>
<tbody>
<tr>
<td>Susan Kohout</td>
<td>Nancy Robillard</td>
</tr>
<tr>
<td>Daniel Austad</td>
<td>Richard Virlee</td>
</tr>
<tr>
<td>Ken Fisher</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1. Security Risk Analysis & Management ................................................................. 1
2. Contingency Plan / Disaster Recovery .................................................................. 2
3. Data Management and Backup .............................................................................. 3
   3A. HIPAA Portable Handheld Device Policy ............................................................ 5
4. System Auditing and Monitoring ....................................................................... 9
   4A. HIPAA Anti-Virus and Patch Management ......................................................... 11
5. HIPAA Security Oversight .................................................................................... 13
6. HIPAA Security Breach Notification for Unsecured Protected Health Information .................................................. 15
   6A. Risk Assessment for Determination of Breach of Protected Health Information .................................................. 20
7. System Access ...................................................................................................... 24
   7A. HIPAA Passwords .......................................................................................... 32
8. HIPAA Business Associate Agreement Policy/Procedure ....................................... 34
9. Facility Access ...................................................................................................... 48
10. HIPAA Facility Maintenance and Repairs ............................................................. 51
11. Re-Use and Disposal of Electronic Media ............................................................ 52
12. Technical Access Controls: Transmission Security, Encryption, and Integrity Controls ........................................... 54
POLICY:
Door County will conduct periodic risk assessments of potential threats and vulnerabilities to the confidentiality, integrity, and availability of its electronic Protected Health Information ("ePHI") and develop strategies to efficiently and effectively mitigate the risks identified in the assessment and analysis process.

PROCEDURE:
1. Door County’s Security Official or designee will ensure risk assessments are conducted to determine potential threats and vulnerabilities to the confidentiality, integrity, and availability of the electronic Protected Health Information ("ePHI").
2. Door County will evaluate whether conditions exist where ePHI could be disclosed without proper authorization, improperly modified, or made unavailable when needed.
3. The risk assessment process will include a review of administrative, technical and physical security safeguards.
4. The risk assessment process will include an analysis of the likelihood that a threat will exploit a vulnerability based upon current controls in place to mitigate the risk.
5. Door County will ensure risk assessments are also conducted for each new and updated hardware or software. Note: Only information security employees or designees can load hardware or software onto/into the information systems.
6. The risk assessment process will include an analysis of the impact of events on the confidentiality, availability, and integrity of ePHI, organizationally sensitive information, and other information system assets.
7. Door County will prioritize, evaluate, and implement security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within the organization given our mission and available resources.
8. Door County will perform periodic technical and non-technical assessments of the Security Rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.
9. Risk assessment data will be maintained for at least 6 years.

REFERENCES:
45 CFR § 164.308(a)(1)(ii)(A) HIPAA Security Rule Risk Analysis
45 CFR § 164.308(a)(1)(ii)(B) HIPAA Security Rule Risk Management
45 CFR § 164.308(a)(8) HIPAA Security Rule Evaluation

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (February 20, 2018)
POLICY:
Door County will have documented disaster recovery plan(s) developed and implemented to ensure recoverability from the loss of data, from systems that collects, maintains, uses or transmits ePHI, due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster.

Door County will have systems, especially those containing Electronic Protected Health Information (ePHI), available during an emergency or a Disaster as needed and feasible to ensuring the confidentiality, integrity, and availability of ePHI.

The Disaster Recovery Plan(s) will include procedures to train the appropriate personnel to implement the disaster recovery plan. The Disaster Recovery Plan(s) will be documented and easily available to the necessary trained personnel at all times to implement the Disaster Recovery Plan.

PROCEDURE:
1. Door County will create and document Disaster Recovery Plan(s) to recover its information systems if they are impacted by a disaster. The plan(s) will be reviewed and revised on an annual basis or more frequently as needed.

2. The Disaster Recovery Plan(s) will include:
   2.1. a. Identification of workforce member responsibilities
   2.2. b. Conditions for activating the plan
   2.3. c. Restoration procedures

3. Door County’s Disaster Recovery Plan(s) will be maintained by Information Security Official.

4. All appropriate Door County workforce members will have access to a current copy of the applicable Disaster Recovery Plan.

REFERENCES:
Regulatory Source:
45 CFR § 164.308(a)(7) HIPAA Security Rule Contingency Plan
45 CFR § 164.308(a)(7)(ii)(B) HIPAA Security Rule Disaster Recovery Plan
45 CFR § 164.308(a)(7)(ii)(C) HIPAA Security Rule Emergency Mode Operation Plan
45 CFR § 164.308(a)(7)(ii)(D) HIPAA Security Rule Testing and Revision Procedure
45 CFR § 164.308(a)(7)(ii)(E) HIPAA Security Rule Applications and Data Criticality Analysis

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (August 21, 2018)
POLICY:
Door County will establish and implement procedures to create and maintain retrievable exact copies of electronic data (including electronic protected health information (ePHI)) to ensure that complete, accurate, and retrievable back-ups of data are available for all technology systems used by the organization, as needed.

Door County will create a retrievable exact copy of sensitive/ePHI data as necessary before movement of equipment and maintain a record/log of movements of Hardware and Electronic Media containing sensitive/ePHI data.

PROCEDURE:
1. Data Backup
   1.1. Detailed procedures describing how to backup data systems are maintained by Technology Services.
   1.2. Individuals responsible for data Backups are trained by individuals experienced on the procedures to complete these Backups or verify the automated Backup was performed.
   1.3. There is a full automated Backup schedule performed on Door County servers at regular intervals based on use, most are completed daily.
   1.4. For all sensitive or ePHI Backups performed on tapes and external hard drives, the media is encrypted.
   1.5. Backups are tested on a periodic basis. Document when files have been completely and accurately restored from the Backup media.
   1.6. Most sensitive/ePHI data Backup is stored through vendors on the cloud.
   1.7. When ePHI Backups are completed and/or stored by a vendor:
      a) The vendors are required to have the above stated controls in place, at a minimum.
      b) A Business Associate Agreement is in place, as required by the Business Associate Policy.
2. Moving sensitive/ePHI – Electronic Media
   2.1. It is not possible or economically practical to control all Electronic Media that enter, leave, and are moved throughout the organization. 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.
   2.2. Users may not remove Workstations, portable devices, or other Hardware or Electronic Media that have sensitive/ePHI data stored on them from the premises, unless authorized by Technology Services or a senior manager. In the event authorization is obtained encryption and other protections are used to secure sensitive/ePHI data.
   2.3. Prior to moving Hardware or Electronic Media that stores or processes ePHI other than those stated above to a new location, said hardware/electronic media should follow the Re-Use and Disposal of Electronic Media Policy or
a) Backup a retrievable copy of the ePHI, when applicable/possible. The individual(s) that creates the Backup also manages the Backup Electronic Media as described in the above Data Backup procedures.

b) Record it on a Certificate of Movement Form.

c) Forward all Certificate of Movement Forms to Technology Services to maintain records in the Inventory Asset List.

2.4. When moving Electronic Media offsite, verify media or data is encrypted, whenever possible.

2.5. Before disposing of Electronic Media at an offsite location, refer to the Re-Use and Disposal of Electronic Media Policy.

REFERENCES:

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 § 134.10(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

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (May 15, 2018)
POLICY:
1. Door County will protect ePHI stored on Portable Handheld Devices from the threat of loss, theft, unauthorized access, or other potential compromises or hazards to Portable Handheld Devices.

2. Prior to the use of Portable Handheld Devices or remote access to ePHI, Workforce Members will be trained on the appropriate safeguards associated with its use.

PROCEDURE:
1. Key Definitions
   1.1 Protected Health Information (PHI) – individually identifiable health information that is received, created, maintained or transmitted by Door County, including demographic information, that identifies a patient, or provides a reasonable basis to believe the information can be used to identify a patient, and relates to:
      • Past, present or future physical or mental health or condition of a patient.
      • The provision of health care to a patient.
      • Past, present, or future payment for the provision of health care to a patient.
   1.2 Electronic Protected Health Information (ePHI) - any PHI that is transmitted by electronic media or maintained in electronic media.
   1.3 Portable Handheld Devices - any mobile, portable, or handheld device that creates, receives, transmits, maintains or stores ePHI. Examples include, but are not limited to, laptop computers, tablets cell/smart phones, SD cards, ultrabook, iPad, PDAs, iPods, iPhones, digital cameras, etc.
   1.4 Sanitize - Complete removal or destruction of, or rendering unavailable, all data on a device or media in a way that prevents someone from retrieving, reading, or reconstructing the data in accordance with National Institute of Standards and Technology ("NIST") standards and the Office of Civil Rights (OCR)'s Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
   1.5 Workforce Members - are employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

2. General Safeguards:
   All Portable Handheld Devices that create, receive, maintain, or transmit ePHI must comply with the following requirements, regardless of whether the Portable Handheld Device is company-supplied or Workforce Member-supplied:
   2.1 Workforce Members shall not access, create, receive, maintain, or transmit ePHI on Portable Handheld Devices unless:
      a. It is permitted by Door County’s “System Access Policy”;
      b. It is necessary for business purposes;
c. The Workforce Member has obtained authorization; and

d. Encryption software is employed for storage and transmission of such ePHI.

2.2 Door County will determine which types of Portable Handheld Devices may be used to create, receive, transmit and maintain PHI, including whether Workforce Members may use Workforce Member-supplied Portable Handheld Devices.

2.3 Portable Handheld Devices must be appropriately secured when not in use. Appropriate security shall include, but is not limited to, physical security, in accordance with Door County’s “System Access Policy,” as applicable, or others methods as determined by Door County.

2.4 ePHI will be stored in secured server environments. If ePHI is stored on a Portable Handheld Device, it should be moved to network drives as soon as possible and removed from the device, where applicable.

2.5 Workforce Members shall not download ePHI to the storage media (e.g., hard drive, solid state drive, etc.) of any Portable Handheld Device unless such device is encrypted or otherwise authorized by Door County.

2.6 Workforce Members shall not print ePHI to a wireless printer using a Portable Handheld Device unless otherwise authorized by Door County.

2.7 Maintain a current and up-to-date anti-malware solution where technically feasible.

2.8 ePHI stored on Portable Handheld Devices shall be Sanitized, disposed of, or destroyed, in the circumstances outlined in, and in accordance with, Door County’s “Re-Use and Disposal of Electronic Media” and procedure.

2.9 Portable Handheld Devices must not be left unattended, or if necessary, must be physically locked away, or secured and hidden from view.

2.10 Workforce Members must promptly report any actual or suspected theft, loss, or cyber threat, or any other potential breach of any Portable Handheld Device on which ePHI is stored to the Door County’s Privacy Officer and Security Officer. This applies regardless of whether the Portable Handheld Device is Workforce Member-supplied or company-supplied. Failure to report may result in disciplinary action. A “remote Sanitization” should be performed or the Portable Handheld Device should be otherwise rendered inoperable, where technically feasible. If stolen, local law enforcement should be notified and a police report obtained and the applicable incident response/breach policy should be consulted.

2.11 Access to ePHI by Workforce Members, business associates, or other entity permitted by law and Door County to access ePHI, is allowable only on a minimum necessary basis and consistent with Door County’s “System Access Policy”.

2.12 The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to ePHI and are extended even after termination or other conclusion of access.

2.13 Door County reserves the right to block, filter or limit access to resources or content if the requesting Portable Handheld Device does not meet the minimum security and technology requirements or if there are any other concerns about the use of such Portable Handheld Device.

2.14 Digital cameras (e.g., stand-alone cameras, smart phone, tablet, etc.) and ePHI captured or maintained by digital cameras shall be subject to the same requirements and restrictions outlined in this policy.

3. Workforce Member-Supplied Portable Handheld Devices
In addition to the general safeguards outlined in Section 2, Workforce Members using their Workforce Member-supplied Portable Handheld Devices must comply with the following requirements:
3.1 Workforce Members may not use their Workforce Member-supplied Portable Handheld Devices to access ePHI unless the Workforce Member is specifically authorized by Door County and only in the manner specified by Door County.

3.2 Workforce Members shall follow all security guidelines, and implement any prescribed security controls when using Workforce Member-supplied Portable Handheld Devices, as required by Door County. Such safeguards shall be substantially similar to those required by company-supplied Portable Handheld Devices.

3.3 Personal applications and/or software used on the Workforce Member's Portable Handheld Devices may not be linked to or synced with work-related applications used to access ePHI, unless approved by Door County.

3.4 Workforce Members are responsible for ensuring that their Portable Handheld Devices are protected from theft, destruction, or unauthorized use and disclosure, and to protect the confidentiality, integrity and accessibility of ePHI.

3.5 When a Workforce Member will no longer be using his/her Portable Handheld Device, the Portable Handheld Device shall be Sanitized in accordance with Door County’s “Re-Use and Disposal of Electronic Media.” Workforce Member shall not sell, trade-in, give away, or throw away his/her Portable Handheld Device without Sanitizing the Portable Handheld Device.

3.6 In addition to other potential sanctions, Workforce Members who violate this policy or other HIPAA policies may have their access to ePHI through their Workforce Member-supplied Portable Handheld Device terminated.

3.7 Door County may, in its discretion, specify mandatory safeguards (such as encryption, password protection, remote wiping, and other administrative controls).

3.8 In order to obtain access to ePHI via a Workforce Member-supplied Portable Handheld Device, the Workforce Member must authorize Door County to Sanitize the Workforce Member's Portable Handheld Device when Door County deems necessary, which may include erasure of personal information.

4. Company-Supplied Portable Handheld Devices
   In addition to the general safeguards outlined in Section 1, company-supplied Portable Handheld Devices must comply with the following requirements:

   4.1 Door County determines which Workforce Members shall have access to company-supplied Portable Handheld Devices and how such Portable Handheld Devices may be used.

   4.2 Door County has established appropriate safeguards and minimum standards for the protection of ePHI on any Portable Handheld Device that may be able to store, process and/or transmit ePHI.

   4.3 Door County shall keep an inventory of all company-supplied Portable Handheld Devices and the Workforce Member to whom it has been issued in accordance with Door County’s “System Access.”

   4.4 In addition to other potential sanctions, Workforce Members who violate this policy or other HIPAA policies may have their company-supplied Portable Handheld Devices confiscated.

   4.5 Door County has the authority to Sanitize any company-supplied Portable Handheld Device, which may include erasure of personal information.

5. Education/Training
   5.1 Door County shall train Workforce Members on appropriate use of Portable Handheld Devices, compliance with the Privacy Rule and Security Rule, and the risks associated with Portable Handheld Devices, such as theft, loss, vulnerabilities, and cyber threats inherent in the use of Portable Handheld Devices.
5.2 Door County shall inform Workforce Members when there are updates or new versions of Portable Handheld Devices are available and shall ensure appropriate implementation of such changes.

REFERENCES:
45 CFR §160.103 HIPAA Definitions
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 §164.310(d)(2)(iii) HIPAA Security Rule Accountability
HIPAA COW Portable Handheld Device Policy

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (July 16, 2019)
POLICY:
Door County will audit access and activity of applications, systems, and networks, including electronic Protected Health Information (ePHI), consistent with available resources.

Door County will implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive data including ePHI.

PROCEDURE:
1. Door County makes reasonable and appropriate attempts to use and obtain systems, applications, and servers containing ePHI with user audit trail reports that can be sorted by user and by patient.
2. If audit reports are not available, or have limited auditing capabilities, the Security Official or designee evaluates whether an upgrade is necessary or if a separate application can be utilized.
3. Auditing efforts are focused on areas of greatest risk, organizational resources, and vulnerabilities as identified in previous incidents, the security risk assessment, and industry trends and events.
4. Door County works with outside web-based vendors, as applicable, to discuss monitoring procedures of audit logs and/or access reports.

User ePHI Access Audits
1. Random user access audits are conducted on a periodic basis to determine if access to ePHI was appropriate for the users' roles.
2. Systems/applications used on a daily basis by multiple users are audited periodically.
3. User audits are also completed in response to:
   3.1. Suspicion that a user has or may be attempting to inappropriately access ePHI, such as from a patient or employee complaint (refer to the Breach Notification Policy).
      a) A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by the Privacy or Security Official and Human Resources Director or designee.
      b) A request for an audit as a result of a patient concern is initiated only by the Privacy Officer and/or Security Official. A copy of the audit information is not shared with patients or their guardians/legal representatives. The Privacy Officer and/or Security Official communicate details of the audit results to the patient as described in the Breach Notification Policy.
   3.2. Selected high risk problem-prone events, such as a VIP encounter (e.g. board member, celebrity, governmental or community figure, etc.).
4. Audit Report Documentation includes the following, when possible:
   4.1. Application, system, server, network, workstation, and patient and/or user audited
   4.2. Audit type
   4.3. Individual/Department that completed the audit
   4.4. Date(s) of audit
   4.5. Reason for the audit
4.6. Conclusions

4.7. Recommendations

4.8. Actions. If it was determined that a breach or other security incident occurred, refer to the Breach Notification Policy.

4.9. Assignments

4.10 Follow-up

Log-in Monitoring

1. Log-in monitoring capabilities are as follows:
   1.1. Information systems, applications, and servers containing ePHI: date and time of each log-on attempt, date and time of each log-off attempt, and user name are on application & system event logs where available,
   1.2. Networks: information on what is operating, penetrations, and vulnerabilities on application & system event logs where available,
   1.3. Workstations used to store or transmit ePHI: date and time of each log-on attempt, date and time of each log-off attempt, user name on Windows security event logs.

2. Log-in attempt reports are reviewed for hackers.

3. Accounts automatically lock after three unsuccessful attempts.

4. If a security incident happened, or is believed to have happened, refer to the Breach Notification Policy.

5. When log-in monitoring is not possible to be done, or the organization decides to not monitor the above mentioned log-in attempts as stated above, the Security Official maintains documentation on the reason/rationale.

REFERENCES:

45 CFR § 164.308(a)(1)(ii)(D) HIPAA Security Rule Information System Activity Review
45 CFR § 164.308(a)(5)(ii)(C) HIPAA Security Rule Log-in Monitoring
45 CFR § 164.312(b) HIPAA Security Rule Audit Controls

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (August 21, 2018)
POLICY:
Door County will guard electronic information systems against viruses and other malicious software.

PROCEDURE:
1. Technology Services has anti-virus/anti-malware software, patches, and firewalls in place to guard against, detect, and report viruses, trojan horses, and worms.

2. The Technology Services Department is responsible for ensuring anti-virus/anti-malware, patches, and firewalls are current, effective, and documented.

3. Anti-virus/anti-malware software is on servers and workstations containing ePHI.
   3.1. Internet - Technology Services maintains applications to filter all internet traffic for threats including viruses, trojan horses, worms, and other malware. Anti-virus/malware software updates applications at least weekly, with additional refreshes during heightened threat activity. Daily updates may be provided by vendors.
   3.2. SPAM - Technology Services maintains a spam-filtering appliance to detect and prevent excessive spam, and virus-laden emails. Technology Services ensures that the filter service is updating frequently.
   3.3. E-mail Antivirus - Technology Services maintains further mail security by scanning all mail for viruses. Technology Services ensures that the appliance is updating frequently.
   3.4. Web Filtering – Technology Services maintains a web filtering appliance to detect and prevent access to websites/services deemed inappropriate or unsafe.
   3.5. Workstations - Technology Services ensures that each workstation has its own antivirus software as a final line of defense. Technology Services ensures that each login prompts the upload of the most current software version.
   3.6. Server updates are automated.
   3.7. Workstation and portable device (computer, laptop, etc.) updates are automated.

4. The Technology Services department is responsible for ensuring patch updates are completed timely.
   4.1. Patch updates that are done manually are evaluated to make sure they should be implemented, so they don't inadvertently cause other problems.
   4.2. Server, workstation, and portable device updates are automated.
   4.3. Networks and servers are secured with a Firewall.
   4.4. Network access is limited to legitimate or established connections.
   4.5. Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment.
4.6. Firewall configurations used to protect networks are approved by the Technology Services Department.

5. Employees must not intentionally introduce and use best efforts to prevent the introduction of other threatening software, viruses, malware, spyware or other destructive applications.

5.1. Users may not open email attachments received from a suspicious sender.

5.2. Users may not download software without approval from the Technology Services Department.

5.3. Portable devices may not be introduced into the private network before the Technology Services Department assesses them for security concerns and approves them for use.

REFERENCES:

Regulatory Source:
45 CFR §164.308(a)(5)(ii)(B) Protection from malicious software

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (February 20, 2018)
POLICY:
Door County is dedicated to maintaining the confidentiality, integrity, and availability of ePHI and protecting it against any reasonably anticipated threats, hazards, and/or inappropriate use or disclosure.
Door County will develop, implement, and oversee the organization’s efforts toward compliance with the Security Rule.
Door County will monitor security policies, procedures, and existing measures, and update them as needed to better protect ePHI.

PROCEDURE:

1. Security Official
Door County will designate a security official who is responsible for the development and implementation of policies and procedures required by the Security Rule and oversee Door County's compliance with the Security Rule.

2. Training
Door County will train members of its workforce on the Security Rule policies and procedures regarding protected health information, as necessary and appropriate for the members of the workforce to carry out their functions within Door County.

3. Documentation
3.1. Door County will maintain all Security Rule related policies and procedures, assessments, and other documentation (such as risk analyses, risk management decisions, moving media, hardware disposal, job descriptions, training, etc.) required by the Security Rule.
3.2. Door County will maintain such documentation for seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.
3.3. Door County will make such documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
3.4. Door County will review such documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

4. Definitions
4.1. Confidentiality
4.2. Integrity
4.3. Availability
4.4. E-PHI
4.5. PHI
4.6. Security Rule
4.7. Privacy Rule
4.8. HIPAA
REFERENCES:
45 CFR §164.308(a)(2) HIPAA Security Rule Assigned Security Responsibility
45 CFR §164.306(a) HIPAA Security Rule General Requirements
45 CFR §164.306(b) HIPAA Security Rule Flexibility of Approach
45 CFR §164.306(e) HIPAA Security Rule Maintenance
45 CFR §164.308(a)(5)(i) HIPAA Security Rule Security Awareness and Training
45 CFR §164.316(a) HIPAA Security Rule Policies and Procedures
45 CFR §164.316(b)(1) HIPAA Security Rule Documentation
45 CFR §164.316(b)(2)(i) HIPAA Security Rule Time Limit
45 CFR §164.316(b)(2)(ii) HIPAA Security Rule Availability
45 CFR §164.316(b)(2)(iii) HIPAA Security Rule Documentation Updates
45 CFR §164.310(a)(2)(iv) HIPAA Security Rule Maintenance Records

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (February 20, 2018)
POLICY:

Door County complies with the regulations for Breach Notification for Unsecured Protected Health Information published in the Federal Register on January 25, 2013 as part of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This Policy sets forth the procedures Door County will use to determine if an impermissible or unauthorized access, acquisition, use or disclosure of Door County's protected health information ("PHI") is a breach for which notification to the affected individual(s) is required under HIPAA.

This Policy applies to Door County and all of its subsidiaries and affiliates. For purposes of this Policy, references to Door County shall be deemed to include sub-units, employees, appointed and elected officials, and group health plan(s).

DEFINITIONS

Capitalized terms not otherwise defined in this Policy shall have the meanings given in HIPAA.

- "Access" means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

- "Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI. An acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated.

Breach excludes:

- Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of Door County or its business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

- Any inadvertent disclosure by a person who is authorized to access Door County’s PHI (whether a Workforce member, business associate, business associate workforce member or other authorized party) to another person authorized to access Door County’s PHI, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

- A disclosure of PHI where Door County or its business associate has a good faith belief that the unauthorized person or entity to whom the disclosure was made would not reasonably have been able to retain such information.

- "Disclosure" means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.
"Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. parts 160 and 164, Subparts A and E, as currently in effect.

"Unsecured PHI" means that PHI of Door County which is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the Department of Health & Human Services ("HHS") in the guidance issued under section 13402(h)(2) of Pub. L.111-5 and available on the HHS website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/br_guidance.html

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Door County or a business associate of Door County, is under the direct control of Door County, whether or not they are paid by the Door County or its business associate.

PROCEDURE:

1. Discovery of Impermissible or Unauthorized Acquisition, Access, Use or Disclosure of Unsecured PHI. All Workforce members and business associates are required to report immediately the discovery of any potentially impermissible or unauthorized acquisition, access, use or disclosure of Unsecured PHI. Reports shall be made to Door County's Privacy Officer. Upon receipt of such report, the Privacy Officer shall begin an investigation, and conduct a risk assessment, to determine whether a Breach has occurred.

2. Investigation. The Privacy Officer shall act as the investigator of the Breach and shall be responsible for the management of the Breach investigation, completion of a risk assessment and coordinating with others at Door County, as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.). The Privacy Officer shall be the key facilitator for all Breach notification processes to the appropriate entities or individuals (e.g., HHS, media, law enforcement officials, etc.).

3. Risk Assessment. For acquisition, access, use or disclosure of Unsecured PHI to constitute a Breach, it must constitute a violation of the Privacy Rule. A use or disclosure of Unsecured PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential Breach. An impermissible or unauthorized acquisition, access, use, or disclosure of Unsecured PHI is presumed to be a Breach unless Door County (or its business associate, as applicable) demonstrates that there is a low probability that the Unsecured PHI has been compromised based on an assessment of at least the following factors:

   3.1. The nature and extent of the Unsecured PHI involved, including the types of identifiers and the likelihood of re-identification (e.g., there is a high probability that the Unsecured PHI has been compromised when detailed clinical information such as treatment plans or diagnosis are involved);

   3.2. The unauthorized person who used the Unsecured PHI or to who the disclosure was made (e.g., there is a low probability that the Unsecured PHI has been compromised when the person who received the Unsecured PHI has an obligation to protect its privacy under HIPAA, such as another covered entity);

   3.3. Whether the Unsecured PHI was actually acquired or viewed (e.g., there is a low probability that the Unsecured PHI has been compromised when forensic analysis indicates that Unsecured PHI on a stolen laptop was never accessed, viewed, acquired, transferred or otherwise compromised); and

   3.4. The extent to which the risk to the Unsecured PHI has been mitigated (e.g., there may be a low probability that the Unsecured PHI has been compromised when an employee, affiliated entity or business associate provides reasonable assurances that Unsecured PHI received in error was immediately destroyed, but reasonable assurances from certain third parties may not be sufficient).
4. **Documentation.**

4.1. The Privacy Officer shall document the risk assessment as part of the investigation and note the outcome of the risk assessment process. Based on the outcome of the risk assessment, the Privacy Officer will determine if there has been a Breach and, if so, provide the appropriate notification to the affected individual(s). The Privacy Officer may make Breach notifications without completing a risk assessment.

4.2. The Privacy Officer, or his or her designee, shall maintain a log of all Breaches. The log shall include the date of the Breach, a description of the impermissible use or disclosure, the date of discovery and the number of individuals affected, if known. The log will also include a description of the types of PHI involved, actions taken to notify individuals, if necessary, mitigate the Breach and prevent future Breaches, and any other information required by HHS.

4.3. All documentation related to the Breach investigation, including the risk assessment and notifications made, shall be retained for a minimum of six years following the date of the incident.

5. **Notification Timing.** Based on the results of the investigation and the risk assessment, the Privacy Officer shall begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of HHS, media outlets, law enforcement officials, etc.). Upon determination that Breach notification is required, the affected individual(s) shall be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach by the Privacy Officer. A Breach shall be treated as “discovered” as of the first day on which an incident that may have resulted in a Breach is known to Door County or, by exercising reasonable diligence would have been known to Door County (or by Door County’s business associate). Door County shall be deemed to have "known" of a Breach if such Breach is known or, if 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 Door County) of Door County.

6. **Delay of Notification Authorized for Law Enforcement Purposes.** If a law enforcement official states to the Privacy Officer that a notification, notice or posting would impede a criminal investigation or cause damage to national security, the Privacy Officer shall delay notification notice or posting:

6.1. For the time period specified by the official, if the statement is in writing and specifies the time for which a delay is required; or

6.2. No longer than 30 days from the date of a verbal statement, unless a written statement as described above is submitted during that time. If the statement is made verbally, the Privacy Officer shall document the statement, including the identity of the official making the statement.

7. **Content of the Notice.** The notice of Breach shall be written in plain language and must contain the following information:

7.1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

7.2. A description of the types of Unsecured PHI that were 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).

7.3. Any steps the individual should take to protect him or herself from potential harm resulting from the Breach.

7.4. A brief description of what Door County is doing to investigate the Breach, to mitigate harm to the individual and to protect against further Breaches.

7.5. Contact procedures for an individual to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.
8. **Methods of Notification.** The method of notification will depend on the individuals or entities to be notified. The following methods must be utilized accordingly:

8.1. **Notice to Individual(s).** Notice shall be provided promptly and in the following form:

8.1.1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If Door 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 personal representative shall be carried out.

8.1.2. **Substitute Notice.** In the case where there is insufficient or out-of-date contact information (including phone number, e-mail address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

8.1.2.1. In a case in which there is insufficient or out-of-date contact information for fewer than ten individuals, then the Privacy Officer will provide the substitute notice by an alternative form of written notice, telephone or other means.

8.1.2.2. In the case in which there is insufficient or out-of-date contact information for ten or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of Door County’s website, or a conspicuous notice in a major print or broadcast media in Door County’s geographic areas where the individuals affected by the Breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the Breach.

8.1.3. If the Privacy Officer determines that 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.

8.2. **Notice to Media.** Notice shall be provided to prominent media outlets serving the state and regional area (of the Breached individuals) when the Breach of Unsecured PHI affects 500 or more individuals of a State or jurisdiction.

8.2.1. The notice shall be provided in the form of a press release.

8.2.2. The Privacy Officer will consider what constitutes a prominent media outlet based upon the State or jurisdiction where Door County’s affected individuals reside. For a Breach affecting more than 500 individuals across a particular state, the Privacy Officer will consider a prominent media outlet to be a major, general interest newspaper with a daily circulation throughout the entire state. The Privacy Officer will not consider a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics), as a prominent media outlet. Where a Breach affects more than 500 individuals in a limited jurisdiction, such as a city, then the Privacy Officer will consider a major, general interest newspaper with daily circulation throughout the city to be a prominent media outlet, even though the newspaper does not serve the whole State.

8.3. **Notice to the Secretary.** Notice shall be provided to the Secretary of HHS as follows:

8.3.1. For Breaches involving 500 or more individuals, the Privacy Officer shall notify the Secretary of HHS as instructed at
8.3.2. For Breaches involving less than 500 individual, the Privacy Officer will maintain a log of the Breaches. The Privacy Officer may report the Breaches during the calendar year or no later than 60 days after the end of that calendar year in which the Breaches were discovered (e.g., 2012 Breaches were to be submitted by 3/1/2013). Instructions for submitting the logged Breaches are provided at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstructio n.html at the same time notice is made to the individuals.

9. **Maintenance of Breach Information/Log.** As described above and in addition to the reports created for each incident, the Privacy Officer shall maintain a process to record or log all Breaches regardless of the number of individuals affected. The following information should be documented for each Breach:

9.1. A description of what happened, including the date of the Breach, the date of the discovery of the Breach and the number of individuals affected, if known.

9.2. A description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, etc.).

9.3. A description of the action taken with regard to notification of individuals, the media and the Secretary of HHS regarding the Breach.

9.4. The results of the risk assessment.

9.5. Resolution steps taken to mitigate the Breach and prevent future occurrences.

10. **Business Associate Responsibilities.** Any business associate of Door County that accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys or otherwise holds, uses or discloses Unsecured PHI shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach, notify the Privacy Officer of such Breach. This notice shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during such Breach. The business associate shall provide the Privacy Officer with any other available information that is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the business associate of discovery of a Breach, the Business Associate will be responsible for notifying affected individual(s), unless otherwise agreed upon by Door County.

11. **Workforce Training.** Door County trains all members of its Workforce on its HIPAA policies and procedures as necessary and appropriate for such persons to carry out their job responsibilities. Workforce members also are trained as to how to identify and promptly report any impermissible or unauthorized acquisition, access, use or disclose of Unsecured PHI. Workforce members that assist in investigating, documenting and resolving Breaches are trained on how to complete these activities.

12. **Non-Retaliation.** It is the Policy of Door County not to retaliate against any Workforce member that makes a good faith report regarding a suspected or actual impermissible or unauthorized acquisition, access, use or disclose of Unsecured PHI, or who assists in investigating, documenting or resolving suspected or actual Breaches.

13. **Sanctions.** Compliance with these policies and procedures is a requirement of employment by, or doing business with, Door County. Workforce members who fail to comply with this policy may be subject to sanctions. Business associates who violate this Policy may be subject to termination.

**REFERENCES:**

**POLICY OWNER:** Security Official

**APPROVED BY:** Door County Administrative Committee (January 21, 2020)
1. Event Information

<table>
<thead>
<tr>
<th>Date Event Occurred: ____________________</th>
<th>Potential Impermissible:</th>
<th>Does Exception Apply? (See Specific Definitions to Apply an Exception)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Event is known: ________________</td>
<td>□ Use</td>
<td>□ Good faith, unintentional by employee/workforce and not further used, etc.</td>
</tr>
<tr>
<td>Person Discovering Event: _____________</td>
<td>□ Disclosure</td>
<td>□ Inadvertent disclosure to another authorized person doing job</td>
</tr>
<tr>
<td></td>
<td>□ Acquisition</td>
<td>□ Recipient could not reasonably have retained the data</td>
</tr>
<tr>
<td></td>
<td>□ Access</td>
<td>□ No</td>
</tr>
<tr>
<td></td>
<td>□ Other</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date Event Reported to Privacy Officer: ____________________</th>
</tr>
</thead>
</table>

Type of Event:

☐ Incidental  ☐ Accidental  ☐ Intentional
☐ Suspected / Unsubstantiated

2. FACTOR 1 - Nature and Extent of PHI Involved (consider with Factor 2)

2.1 PHI involved: __________________________________________

2.2 # of Identifiers in PHI: __________________________________

2.3. Type of identifiers: ______________________________________

2.4. Can PHI be used to re-identify patient(s)?  ☐ Yes  ☐ No

2.5. Can PHI be combined with other available info & used to re-identify patient(s)?  ☐ Yes  ☐ No

2.6. Number of patients affected: ____________________________

- The more identifiers, the more chance a patient can be re-identified.
- Is PHI more sensitive in nature, such as credit card #’s, SSN’; or other information that increases the risk of identity theft or financial fraud, treatment plan, diagnosis, meds, history, test results?
- Could this information be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient’s own interests?
- Is there likelihood that PHI can be re-identified based on the context and the ability to link the information with other available information.

For example, a list of pt names, addresses and hospital ID numbers are obviously identifiable and there is more than a low probability that the information has been compromised, but also consider Factor 2.

However would an unauthorized recipient have the ability to combine a list of patient discharge dates and diagnoses with other information available to re-identify patient?
2.7. Was Identifiable PHI Involved?  □ Yes    □ No

3. FACTOR 2 – People Involved (Consider with Factor 1)

3.1. Who impermissibly used/disclosed PHI?
________________________________________________

3.2. Date: __________________________

3.3. Unauthorized person/entity who acquired/received PHI:
________________________________________________

3.4. Does unauthorized person/entity have obligation to protect privacy & security of PHI?
□ Yes  □ No

- If unauthorized person or entity has an obligation to protect privacy and security of PHI, then probability that information will be compromised is lower, but also consider Factor 1

3.5. Did the person have an obligation to protect PHI?  □ Yes    □ No

4. FACTOR 3 – Acquired or viewed?

4.1. Was PHI actually obtained/received or did only the opportunity exist to obtain/receive PHI?
________________________________________________

4.2. Was PHI actually viewed or did only the opportunity exist to view PHI?
________________________________________________

- If PHI was obtained or received but not viewed, then perhaps the probability is low that the PHI was compromised. For example, if a laptop was stolen and then returned and a forensic analysis proved that PHI had not been accessed, then PHI would not have been actually acquired or viewed.

4.3. Did the person view the PHI?  □ Yes    □ No

5. FACTOR 4 – Mitigation

5.1. To what extent has the risk to the PHI been mitigated?
________________________________________________

5.2. Have you obtained assurances that PHI will not be further used or disclosed (confidentiality agreement, etc.)?
________________________________________________

5.3. Will PHI be destroyed (attestation signed)?
________________________________________________
We note that this factor, when considered in combination with the factor regarding the unauthorized recipient of the information discussed above, may lead to different results in terms of the risk to the protected health information. For example, a covered entity may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient.

5.4. Did we get the PHI back?  ☐ Yes  ☐ No

OTHER FACTORS:

6. DETERMINATION
6.1. What is the overall probability that PHI has been compromised?
☐ Low  ☐ Medium  ☐ High

7. NOTIFICATION
7.1. Is breach notification, by organization or another covered entity, to patients required?
☐ Yes  ☐ No
7.2. Is breach notification, by organization or another covered entity, to media required?
☐ Yes  ☐ No
7.3. Is breach notification, by organization or another covered entity, to HHS required?
☐ Yes  ☐ No
7.4. If yes, when?
☐ Immediate  ☐ Year end
7.5. Has law enforcement asked organization for a delay of the notification?
☐ Yes  ☐ No

Privacy Officer Signature  Date
________________________________________  ____________________________

8. Does Exception Apply? (See Specific Definitions to Apply an Exception)
8.1. ☐ Good faith, unintentional by employee/workforce and not further used, etc.

Example- A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it. The billing employee unintentionally accessed protected health information to which he was not authorized to have access. However, the billing employee’s use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule.
In contrast, a receptionist at a covered entity who is not authorized to access protected health information decides to look through patient files in order to learn of a friend’s treatment. In this case, the impermissible access to protected health information would not fall within this exception to breach because such access was neither unintentional, done in good faith, nor within the scope of authority.

8.2. Inadvertent disclosure to another authorized person doing job

Example, this exception encompasses circumstances in which a person who is authorized to use or disclose protected health information within a covered entity, business associate, or organized health care arrangement inadvertently discloses that information to another person who is authorized to use or disclose protected health information within the same covered entity, business associate, or organized health care arrangement, as long as the recipient does not further use or disclose the information in violation of the Privacy Rule.

8.3. Recipient could not reasonably have retained the data

For example, a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as breaches.

As another example, a nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the protected health information from the patient. If the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.
POLICY:
Door County will safeguard the confidentiality, integrity, and availability of electronic protected health information (ePHI), other sensitive information, and business and proprietary information within its information systems by controlling access to these systems/applications. Access to information systems by all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable based upon job function and duties.

PROCEDURE:
1. Access Establishment and Modification
   1.1 All requests for access to any of Door County’s information systems and applications must be accompanied with a signed “Confidentiality and Information Access Agreement” form (see Appendix 1) and the “System Access Request/Change” form (See Appendix 2) approved by the Security Official or designee.
      a) Access will not be granted until signed “Confidentiality and Information Access Agreement” and "System Access Request/Change” forms are received, reviewed, and additional approval is obtained if required.
      b) Training related to security, confidentiality, and incident reporting must occur when log in credentials are issued.
      c) The “Confidentiality and Information Access Agreement” and the “System Access Request/Change” forms are maintained by the Human Resources Department.
   1.2 Department Head or designee are responsible for notifying Human Resources of employees transferred into a new department or new role and facilitating completion of the “System Access Request/Change” form and forwarding it to the Security Official.
      a) The Security Official or designee is responsible for changing the user’s access to information systems based on the user’s new role within 5 business days of notification.

2. Workforce Clearance Procedures
   2.1 The level of security assigned to a user to the organization’s information systems is based on the minimum necessary information (amount of data) access required to carry out legitimate job responsibilities assigned to a user’s job classification and/or to a user needing access to accomplish the intended purpose of disclosure.
   2.2 Any access not specifically authorized is prohibited.

3. Access Authorization
   3.1 Role based access categories for each information system/application are pre-approved by Security Official or designee. Categories are defined by the importance of the applications running on the information system, the sensitivity of the ePHI or other information on the information system, security controls on the information system, security controls on the workstation utilized to access the information system, and the extent to which the information system is connected to other information systems. Any access must be based on the minimum necessary information needed for the user’s role.
   3.2 The Security Official or designee grants the level of access to users based on these pre-determined categories.
3.3 Refer to the remote access policy for details relating to remote access.

4. Person or Entity Authentication
   4.1 Each user has and uses a unique User Login ID and password that identifies him/her as the user of the information system.

5. Unique User Identification
   5.1 Access to the organization’s information systems/applications is controlled by requiring unique User Login ID’s and passwords for each individual user.
   5.2 Password requirements should be based on current industry NIST standards whenever possible (for example 8 character minimum with upper and lower case letters and numbers) (See Password Policy).
   5.3 Passwords are not displayed at any time. Password characters are replaced with asterisks “*” or other characters when typed.
   5.4 Users should not select passwords that may be easily guessed or obtained using personal information (i.e., names, favorite sports team, etc.) (Refer to Password Policy).
   5.5 The Security Official or designee assigns a User Login ID and generic password for each user to utilize for first time access into each information system. The User Login ID and password are forwarded to the user securely (e.g., verbally).
   5.6 Each information system automatically requires users to change their password upon first-time use of the information system.

6. Password Management (See Password Policy)
   6.1 User Login IDs and passwords are used to control access to the organization’s information systems and should not be disclosed. Under rare circumstances the Security Official or designee, may need a user ID and password. When that happens the password may be shared but should be changed to a new password as soon as possible. This is the ONLY person you should ever disclose your password to.
   6.2 Users may not allow anyone for any reason to have access to any information system using another user’s unique User Login ID and password with the exception of the Security Official or designee as outlined above.
   6.3 Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization.
   6.4 The information systems are programmed to deny user’s ability to use up to 10 prior passwords whenever possible.
   6.5 Users that do not recall their password may contact Technology Services who in turn provides the employee with a temporary, one-time use password which must be changed on first use. Users may also use the Password Self Service Tool to reset their password.
   6.6 Passwords are inactivated upon an employee’s termination (refer to the termination procedures in this policy).
   6.7 If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the Security Official or designee.

7. Automatic Logoff
   7.1 Users are required to make information systems inaccessible by any other individual when unattended by the users locking or logging off the systems.
   7.2 Users must log off or disconnect from information systems/applications at the end of their shift, or at the end of their need to use the system/application, whichever is sooner.
   7.3 Technology Services should automatically lock or logoff systems after at a minimum 20 minutes of inactivity. Shortened automatic log off times should be implemented for workstations located in public or high traffic areas or for portable devices. Each organization must choose the number of minutes for automatic logoff based on its risk analysis.
   7.4 The Security Official or designee can approve exceptions to automatic log off requirements.

8. Workstation Use
   8.1 Workstations should only be used for authorized business purposes.
   8.2 When possible workstations should be placed in secure areas. Workstations in public areas must be logged off or locked when not in use or limited access given. Users must take actions
to prevent unauthorized viewing (e.g. privacy screens, minimizing sessions, closing laptops, and so on).

8.3 All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI and other sensitive, business or proprietary information in the information systems at all times.

8.4 Workstations may not be used to engage in any activity that is illegal or is in violation of organization’s policies.

8.4.1 Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or “X-rated”. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual’s race, age, disability, religion, national origin, physical attributes, sexual preference, political affiliation, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization’s system.

8.4.2 Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization’s best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.

8.4.3 Solicitation of non-company business, or any use of organization’s information systems/applications for personal gain is prohibited.

8.4.4 Participation in chain letters and other such activities is also prohibited.

8.4.5 Transmitted messages may not contain material that criticizes organization, its providers, its employees, or others.

8.4.6 Users may not misrepresent, obscure, suppress, or replace another user’s identity in transmitted or stored messages.

9. Termination Procedures

9.1 Department Heads or designee are required to notify Human Resources Director or designee upon completion and/or termination of access needs and facilitating completion of the “Termination Checklist” (see Appendix 4).

9.2 Human Resources Director or designee will notify the Technology Services Director or designee Department to terminate a user’s access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and are filed with the Human Resources Director and Privacy Officer):

9.2.1 The user has been using their access rights inappropriately,

9.2.2 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)

9.2.3 An unauthorized individual is using a user’s 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).

9.3 Technology Services Director or designee will terminate users’ access rights immediately upon notification.

9.4 Technology Services Director or designee may terminate access of users that have not logged into organization’s information systems/applications for a period of over six (6) months.

REFERENCES:
45 CFR §164.308a4iiC HIPAA Security Rule Access Establishment and Modification
45 CFR §164.308(a)(3)(i) HIPAA Security Rule Workforce Security
45 CFR §164.308(a)(3)(ii)(A) HIPAA Security Rule Authorization and/or Supervision
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)(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(d) HIPAA Security Rule Person or Entity Authentication
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

POLICY OWNER:  Security Official

APPROVED BY: Door County Administrative Committee (August 21, 2018)
Door County is dedicated to safeguarding and maintaining the confidentiality, integrity, and availability of our patient, employee, and proprietary information (collectively “Confidential Information”) regardless of whether the information is written, electronic or verbal.

- **Patient information or protected health information** (“PHI”), is any personal, or medical information that relates to a patient’s treatment, payment, or the health care operations of Door County.
- **Employee records** include information about employees’ salaries, benefits, performance reviews, medical information and other human resources’ matters.
- **Proprietary information** is private (not publically available) information about Door County’s operations, associates, plans, development, financial information, strategies, purchasing, marketing, etc.

This Confidentiality and Information Access Agreement (“Agreement”) is required to be read, signed, and complied with by all users as a condition of access to any information system. The user signing this Agreement may only access, use, and disclose Confidential Information as needed to perform his/her job responsibilities as allowed by law, organization policies and procedures, and/or as agreed upon between the user and Door County.

Such obligations continue after the individual is no longer employed by Door County.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>I understand and agree that I must safeguard and maintain the confidentiality, integrity, and availability of all Confidential Information I use, disclose, and/or access at all times, whether or not I am at work and regardless of how it was accessed.</td>
</tr>
<tr>
<td>2.</td>
<td>I understand that access to all Door County systems or devices, including Email and Internet, are intended for business usage.</td>
</tr>
<tr>
<td>3.</td>
<td>I will only access, use, and/or disclose the minimum necessary Confidential Information needed to perform my assigned duties and disclose it to other individuals/organizations who need it to perform their assigned duties or as allowed by law. PHI is specifically protected, by law, from further disclosures without prior authorization.</td>
</tr>
<tr>
<td>4.</td>
<td>I will only access or use the systems or devices that I am authorized to access and agree not to demonstrate the operation or function of any of Door County systems or devices to unauthorized individuals.</td>
</tr>
<tr>
<td>5.</td>
<td>I will not access my own, or my family’s, PHI in any system without prior Authorization from the Technology Services Director (unless required to perform my job responsibilities).</td>
</tr>
<tr>
<td>6.</td>
<td>I will not use tools or techniques to break/exploit security measures.</td>
</tr>
<tr>
<td>7.</td>
<td>I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.</td>
</tr>
<tr>
<td>8.</td>
<td>I will not connect to unauthorized networks through Door County systems or devices.</td>
</tr>
<tr>
<td>9.</td>
<td>I will not download, copy, store, transmit or replicate any PHI from Door County’s information systems to store or use on any other system or other portable media or devices or to any unauthorized user, except in situations whereby explicit approval to do so has been granted by Door County’s Technology Services Director or designee with prior review by the HIPAA Security Official &amp; Privacy Officer. If I received this approval to download data I will assume sole and absolute responsibility to manage and protect it based upon standards listed in this Agreement and according to the law.</td>
</tr>
<tr>
<td>10.</td>
<td>I understand that I have neither ownership interest nor expectation of privacy in any information accessed or created by me during my relationship with Door County. Door County may audit, log, access, review, and otherwise utilize information stored on or passing through its systems for many reasons, including to maintain the confidentiality, integrity, and availability of Confidential Information.</td>
</tr>
</tbody>
</table>
11. I will not install any software program onto Door County equipment without prior written approval from the Technology Services Director.

12. I will not use Door County’s information systems to create, receive, maintain or transmit any communications consisting of discriminatory, harassing, obscene, solicitation, or criminal information.

13. I understand that my User Login ID(s) and password(s) are confidential and used to control access to Door County’s information systems and an electronic signature(s) is the equivalent to my legal signature. I will not disclose my user ID or password to anyone nor allow anyone to access any information system using my User Login ID(s) and password(s) for any reason.

14. I will immediately report to Door County’s Security Official any activity that violates this agreement, Confidential Information laws, or any other incident that could have any adverse impact on Confidential Information.

15. I understand that I will be held accountable for all inquiries, entries, and changes made to any Door County’s information system using my User Login ID(s) and password(s).

16. I will continue to maintain the confidentiality, integrity, and availability of all Confidential Information even after termination, completion, cancellation, expiration, or cessation of access to Door County’s information systems.

17. I will only use my officially assigned, personal User Login ID(s) and password(s).

18. I agree to return any original and/or copied records and documents containing Confidential Information as well as any organizational keys, identification/access cards (badges), phones, wireless access devices, computers or any other device that would provide access to Door County or its information systems.

19. I will immediately notify Door County’s Security Official or designee if my password has been seen, disclosed, or otherwise compromised.

20. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment or business relationship, suspension and loss of privileges, termination of authorization to work within Door County, as well as legal actions.

Refer any questions related to this Agreement to the HIPAA Security Official or the Privacy Officer.

By signing this Agreement, I agree that I have read, understand and will comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

User Name (Print) ______________________ User Signature ______________________ Date ______________

Please return this completed Agreement to: Human Resources Director
Appendix 2

DOOR COUNTY

SYSTEM ACCESS REQUEST/CHANGE FORM

Complete this form and send to Human Resources Director and Technology Services Director or designee(s).

Employee Name _______________________________      Emp. # __________________

Date ________________

Job Title ______________________________________     Current Department

____________________________

CHOOSE ONE:

☐ This is a new employee       Start Date: ______/_____/______

☐ This is a change in a current employee’s department/responsibilities       Yes (New Department) ________________ / No

Is this employee replacing another employee?       Yes (Whom)__________________________ / No

☐ This is an employee termination Yes/No       Last Worked Day _____/_____/________

Place an ‘X’ by the application that the employee needs access to or access removed

Microsoft Word/Excel/Power Point

Microsoft Outlook

Place an ‘X’ by the tools needed or to be collected

Telephone

Additional Personal Computer – Desktop/Laptop

Voice Mail

Please write below the ‘H’ drive shared folders/subfolders the employee needs access to or removal from - department & committee specific

Department Head’s Signature: _____________________________

Date: ___________________

Please answer the following questions so we can Accurately set up the employee.

1. Brief description of job duties-

2. Will the employee need a pc for their position? If yes, is there one at the workstation now?

Department Head’s Signature: _____________________________
Appendix 3
Termination Checklist

Follow appropriate policies and procedures for personnel replacement, responsibility transitions, benefit and insurance changes, etc. The following checklist is to be used to safeguard access to confidential information when employment ends at Door County.

<table>
<thead>
<tr>
<th>Date of Termination</th>
<th>Employee</th>
<th>Title</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Termination</th>
<th>Voluntary</th>
<th>Involuntary</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Responsible Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Collect Employee’s Identification Badge/Access Card</td>
<td>Department Head</td>
</tr>
<tr>
<td>Collect Employee’s Keys (e.g., building, department, desk, file cabinets, etc.)</td>
<td>Department Head</td>
</tr>
<tr>
<td>Delete All Building Access Codes</td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td></td>
</tr>
<tr>
<td>Transfer Employee’s Files</td>
<td></td>
</tr>
<tr>
<td>Telecommunications</td>
<td></td>
</tr>
<tr>
<td>Terminate Employee’s Voice Mail</td>
<td></td>
</tr>
<tr>
<td>Collect Employee’s Cell Phone (if applicable)</td>
<td></td>
</tr>
<tr>
<td>Information Systems</td>
<td></td>
</tr>
<tr>
<td>Terminate Employee’s E-Mail Account</td>
<td></td>
</tr>
<tr>
<td>Terminate Employee’s Access to Other Programs:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Collect Employee’s Organization Owned Mobile Devices</td>
<td>Department Head</td>
</tr>
</tbody>
</table>

Completed By
(Name/Title)

Date
POLICY:
This policy outlines the creation, use, changing and safeguarding of passwords used to gain access to technology resources belonging to the County of Door. Passwords are the entry point to Door County's technology resources. Protecting access to these resources is crucial to ensuring that Door County systems remain secure. Door County must be diligent in guarding access to its resources and protecting them from threats both inside and outside of County Government. The objective is to enable employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs of Door County.

PROCEDURE:
1. Systems Involved and Frequency of Change:
   1.1 Network connection: Windows username and password will automatically be prompted at a login to change the password every eight weeks.
   1.2 AIX/Unix password: Users of the Door County Public Safety system will automatically be prompted to change their password every eight weeks.
   1.3 AS400 profile password: All IBM AS400 users will be prompted to change their profile password every eight weeks.
   1.4 Voicemail password: This password does not have an automatic expiration but it is recommended that users change this password at least once every six months.
   1.5 Third party applications: Contact the Technology Services Department employee acting as the administrator for the application to determine specific password requirements. For example _TCM, NWS, or Spillman_______________.
2. State Applications: Contact your State representative for specific password requirements.
3. Internet Applications: These applications may or may not have password requirements. Contact the application or service provider for specific password requirements. For example _NeoGov, CHEMS, or Image Trend_______________.
4. Computer BIOS Password: The password for hardware-level access to your computer will not automatically change and shall be controlled by Technology Services personnel ONLY.
5. Password Usage:
   5.1 Passwords for all systems are subject to the following rules:
      5.1.1 No passwords are to be shared, or in any way made known to anyone other than the user involved. This includes supervisors and/or department heads.
      5.1.2 No passwords are to be shared in order to replace an employee who is out of the office. The employee's supervisor shall contact the Technology Services Department and request a temporary account or appropriate changes to
permissions if there are resources that the person needs to access.

5.1.3 Passwords are not to be displayed or concealed anywhere in the employee's workspace.

5.1.4 A minimum of ten unique passwords must be used before the first password can be repeated.

6. Password Composition:

6.1 The same password for all accounts and logins is impossible. Between the State, County, and third-party applications multiple passwords are an unfortunate reality. The following sections provide rules for passwords on the County's Windows domain, Unix server, and AS400. If an employee needs access to any other application they are using and not mentioned in the previous sentence, they should contact the administrator of that system and follow the password rules of that system.

6.2 User passwords must meet the following minimum criteria:

6.2.1 Passwords should not contain the employee's name, address, date of birth, username, nickname, or any term that could easily be guessed by someone who is familiar with the employee.

6.2.2 Password must be at least eight characters long.

6.2.3 Password shall contain no repeated characters side by side.

7. Additional Requirements:

7.1 Use both upper and lower case letters.

7.1.1 Most systems accept upper and lower case and those that do not will just ignore the letter's case.

7.2 Use numbers in the password.

7.3 Use non-alphanumeric characters (symbols)

7.3.1 The AS400 system only allows the #, $, _ (underscore), and @ symbols.

7.4 After three failed attempts to log in, the County systems will lock the user out until the Technology Services Department is contacted and unlocks the account. State and third party applications may have other security lockout procedures. If you are in doubt, contact the administrator or State representative for that system.

REsponsibilities:

Technology Services Department has the responsibility to administer and enforce this policy. Enforcement will be through systematic means and interaction with technology users. All Door County personnel are responsible for complying with this policy. Failure to comply with this policy will subject an employee to disciplinary action up to and including termination of employment.

SUPPORT:

All Door County computer users are to contact the Technology Services Department staff for support of the password.

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (May 15, 2018)
POLICY:
Door County will obtain business associate agreements as required by HIPAA.

PROCEDURE:
Door County’s Security Official shall be responsible for overseeing the management of BA relationships and BAA s. Door County’s departments/business units are responsible for assessing existing and future vendor/business relationships to determine whether a BAA is needed (See Appendix 1).

1. Determining a Need for a BAA
1.1 Door County may determine the need for BAAs through a variety of methods, including:
   - Mapping the flow of PHI and identifying where PHI is created, received, maintained, or transmitted to or by external entities.
   - Reviewing contract management documents/software and identifying where PHI is created, received, maintained, or transmitted to or by external entities.
   - Reviewing 1099 tax forms to identify vendors with business arrangements under which PHI is created, received, maintained, or transmitted to or by vendors.
   - Assessing new vendor/business arrangements to determine if PHI will be created, received, maintained, or transmitted.

1.2 A BAA is required under the following circumstances:
   - The vendor’s staff members are not members of Door County’s Workforce; and
   - The vendor is performing a service or function for or on behalf of Door County; and
   - That “service or function” involves the creation, receipt, maintenance, transmission, access, storage, use, or disclosure of PHI.

1.3 A BAA is not required in the following circumstances:
   - Disclosures by a CE to a health care provider concerning the treatment of an individual;
   - Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of 45 CFR § 164.504(f) apply and are met; and
   - Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

2. Necessary Business Information
2.1 When Door County has determined that a BA relationship exists (or will exist for a new vendor/business arrangement), the relevant department/business unit leader shall contact Door County’s Security Official to initiate a BAA. The department/business unit leader shall provide the following information to “customize” the BAA:

- The name and contact information of the BA.
- A description of the type of service(s) being provided by the BA, which should be consistent with the underlying services agreement (if any). Include a copy of the underlying services agreement with the BA (if any).
- Consistent with the service(s) being provided by the BA, list all permitted uses and disclosures of PHI.
- The name of [Organization Name]’s department/business unit and leader responsible for the BAA.
- Date BA will begin creating, receiving, maintaining or transmitting PHI.
- Contact information for the operational contact and Privacy Officer of BA.
- Any additional BAA provisions requested by Door County (See Procedure 7 below).

3. Underlying Agreement

3.1 If a vendor/business relationship requiring a BAA is in the contract negotiation and development phase, the provisions of the BAA may be incorporated into the contract as an option (a separate BAA would not be legally required).

4. Mandatory Terms

4.1 Obligations and activities which must be addressed in the BAA document are listed in Appendix 2.

5. Contact/Notification

5.1 Door County documents the contact person for any reporting that may need to occur under the BAA.

- Name of the Entity:
- Attn:
- Address:
- City, State, Zip
- Phone:
- Fax:
- e-mail:

6. Term of BAA

6.1 The BAA shall be effective for the length of the relationship between the BA and Door County, unless otherwise terminated under the provisions outlined in the BAA. Similarly, it is highly encouraged that any BAA contain a “survivability” clause indicating that certain provisions of the BAA (such as those governing protection of PHI that cannot be returned or destroyed immediately upon BAA termination) will remain in effect indefinitely, even once the agreement and/or relationship have terminated.

7. Termination

7.1 If Door County chooses to terminate the arrangement with its BA or the BA chooses to terminate the arrangement with Door County, any relevant underlying agreement may be terminated as
outlined in the BAA. Please note, HIPAA requires only that the BAA outline termination options for the CE. While mutual termination may be included in BAAs, this is not required under HIPAA. Upon termination of the BA relationship, Door County and responsible department/business unit leader, in conjunction with the Privacy Officer shall confirm that return/destruction requirements are completed by the BA.

8. Other BAA Terms

8.1 In addition to the required BAA provisions outlined in Appendix 2, Door County may consider addressing some or all of the following considerations in its BAAs:

- Insurance responsibilities (e.g., cyber insurance).
- Limitation of Liability.
- Indemnification requirements.
- Financial risk (e.g., breach notification, mitigation).
- Offshoring PHI (including any relevant Medicare Advantage considerations).
- Audit rights.
- De-identification of PHI.
- Subcontractor selection.
- Network/software access standards.
- Door County shall consider whether to acknowledge that the Security Incident reporting section in the BAA constitutes notice by the BA to the CE that attempted but unsuccessful Security Incidents (such as pings, broadcast attacks on BA’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above which regularly occur) and that no further notice will be made by the BA unless there has been a successful Security Incident. The BA should be prepared to cooperate with the CE with the provision of information needed surrounding a successful breach so the CE can meet its reporting and notification requirements.

9. Additional Considerations

9.1 With each vendor/business relationship, Door County considers to what extent it wishes to review and monitor the activities of its BA. As clarified in the HIPAA Omnibus Rule, CEs must ensure that (1) BAs are safeguarding PHI and using and disclosing the information only as permitted or required by the Privacy Rule and, similarly, (2) that there are “satisfactory assurances” that BAs are appropriately safeguarding ePHI created, received, maintained, or transmitted on behalf of the CE, per the Security Rule. Ultimately, the obligation to notify individuals of breaches of unsecured PHI and take reasonable steps to cure any potential breach and/or end the violation rests both with the BA (and its Subcontractors depending on BAA requirements) and the CE, both of which are now subject to civil monetary penalties for certain HIPAA violations and directly liable to the U.S. Department of Health and Human Services Office for Civil Rights for violations of HIPAA.

For each vendor/business relationship, Door County considers monitoring obligations and responsibilities in conjunction with the common law principle of agency in order to assess what level of control Door County wishes to exert on its BA relationship.

In addition, for each vendor/business relationship, Door County considers the complexity, experience, and capabilities of the vendor in order to guide the level of involvement in review, monitoring, audits, etc. In general, complex entities that are familiar with HIPAA compliance requirements (e.g., vendor is a covered entity, large insurance company, or electronic medical records vendor) are less likely to need significant monitoring. However, businesses that are newly subject to HIPAA compliance requirements due to the expansion of the definition of a “business associate” under HIPAA may require more monitoring. This assessment shall be
conducted by the Door County Privacy Officer, Security Officer and responsible business unit/leader.

10. Contracting as the Downstream Party in a BAA

10.1 When entering into a BAA as a BA, Door County should:
   • Forward the external information to Door County’s Privacy Officer to review the submitted BAA to ensure that the provisions outlined are consistent with those set forth in this policy or as documented on the attached (See Appendix 2). If the BAA terms are consistent with legal requirements and reasonable for Door County the Privacy Officer may recommend signing the BAA as written.
   • If the BAA is not consistent with this policy or contains additional provisions or provisions that are inconsistent with HIPAA, the Privacy Officer may recommend any or all of the following alternatives.
     • Suggest any necessary additional provisions and sign the BAA as amended.
     • Suggest removal of unnecessary or impracticable provisions and sign the BAA as amended.
     • Refer the BAA to legal counsel to determine whether the terms are reasonable and meet all legal requirements before signing.

11. Documentation

11.1 To meet documentation requirements of the Security Rule, the responsible individual/team maintains a file/electronic spreadsheet of BAAs. This file includes the following information, as appropriate, and be available for review as needed:
   • Name of CE/BA.
   • Description of Door County’s operations with which the vendor is involved.
   • Effective date and term of underlying agreement (if applicable).
   • Date BAA signed by Door County and vendor.
   • Location of BAA within Door County and responsible department/business unit leader.
   • Any additional notes, such as the next scheduled review date.

12. Definitions

12.1 Business Associate ("BA")
12.2 Business Associate Agreement ("BAA")
12.3 Covered Entity ("CE")
12.4 E-PHI
12.5 IIHI
12.6 PHI
12.7 Subcontractor
12.8 Workforce

REFERENCES:

45 CFR § 164.308(b)(1) Security Rule Administrative Safeguards: Business Associate Contracts and Other Arrangements
45 CFR § 164.314 Security Rule: Organizational Requirements Business Associate Contracts or Other Arrangements
45 CFR § 164.316 Security Rule: Policies and Procedures and Documentation Requirements
45 CFR § 164.410 Breach Notification: Rule Notification by Business Associates
45 CFR §§ 164.502(a)(3)-(5) and (e)(1) Privacy Rule Uses and Disclosures of Protected Health Information: General Rules and Disclosures to Business Associates
45 CFR §§ 164.504(e)(1)-(5) Privacy Rule Uses and Disclosures Organizational Requirements: Business Associate Agreements and Business Associate Agreements with Subcontractors

HIPAA COW Business Associate Agreement Policy/Procedure

**POLICY OWNER:** Security Official

**APPROVED BY:** Door County Administrative Committee (**July 16, 2019**)
## APPENDIX 1: EXAMPLES OF BUSINESS ASSOCIATES

### EXAMPLES OF BUSINESS ARRANGEMENTS THAT MAY INVOLVE DISCLOSURE OF PHI & REQUIRE BAA/ADDENDUMS OR CONTRACT PROVISIONS

<table>
<thead>
<tr>
<th>Accrediting/Licensing Agencies (e.g., TJC)</th>
<th>Pathology Services Contracts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Consultants/Vendors</td>
<td>Paper Recycling Contracts</td>
</tr>
<tr>
<td>Actuarial Consultants/Vendors</td>
<td>Patient Satisfaction Survey Contracts</td>
</tr>
<tr>
<td>Agents/Contractors Creating, Receiving, Maintaining, Transmitting, Accessing, Using or Disclosing PHI (e.g., Consultants)</td>
<td>Payer-Provider Contracts (Provider for Health Plan)</td>
</tr>
<tr>
<td>Application Service Providers (e.g., prescription mgmt.)</td>
<td>Physician Billing Services</td>
</tr>
<tr>
<td>Attorneys/Legal Counsel</td>
<td>Physician Contracts (non-employed providers)</td>
</tr>
<tr>
<td>Auditors</td>
<td>Practice Management Consultants/Vendors</td>
</tr>
<tr>
<td>Benchmarking Organizations</td>
<td>Professional Services Contracts (e.g., Medical Directors)</td>
</tr>
<tr>
<td>Benefit Management Organizations</td>
<td>Quality Assurance Consultants/Vendors</td>
</tr>
<tr>
<td>Claims Processing/Clearinghouse Agency Contracts</td>
<td>Radiology Services Contracts</td>
</tr>
<tr>
<td>Coding Vendor Contracts</td>
<td>Record Copying Service Vendor Contracts</td>
</tr>
<tr>
<td>Collection Agency Contracts</td>
<td>Record Storage Vendors</td>
</tr>
<tr>
<td>Computer Hardware Contracts</td>
<td>Release of Information Service Vendor Contracts</td>
</tr>
<tr>
<td>Computer Software Contracts</td>
<td>Record Copying Service Vendor Contracts</td>
</tr>
<tr>
<td>Consultants/Consulting Firms</td>
<td>Record Storage Vendors</td>
</tr>
<tr>
<td>Data Analysis Consultants/Vendors</td>
<td>Release of Information Service Vendor Contracts</td>
</tr>
<tr>
<td>Data Transmission Providers (PHI involved)</td>
<td>Repair Contractors of Devices Containing PHI</td>
</tr>
<tr>
<td>Data Warehouse Contracts</td>
<td>Revenue Enhancement/DRG Optimization Contracts</td>
</tr>
<tr>
<td>E-Prescribing Gateway</td>
<td>Risk Management Consulting Vendor Contracts</td>
</tr>
<tr>
<td>Emergency Physician Services Contracts</td>
<td>Shared Service/Joint Venture Contracts with Other Healthcare Organizations (No PHI involved)</td>
</tr>
<tr>
<td>Health Information Organization</td>
<td>Statement Outsource Vendors</td>
</tr>
<tr>
<td>Hospitlist Contracts</td>
<td>Telemedicine Program contracts</td>
</tr>
<tr>
<td>Insurance Contracts (e.g., Coverage for Risk, Malpractice, etc.)</td>
<td>Third Party Administrators</td>
</tr>
<tr>
<td>Interpreter Services Contracts</td>
<td>Transcription Vendor Contracts</td>
</tr>
<tr>
<td>IT/IS Vendors</td>
<td>Waste Disposal Contracts (e.g., Hauling, Shredding)</td>
</tr>
<tr>
<td>Legal Services Contracts</td>
<td><strong>Health Plan Relationships:</strong></td>
</tr>
<tr>
<td>Medical Staff Credentialing Software Contracts</td>
<td>Pharmaceutical Benefits Management Contracts</td>
</tr>
<tr>
<td>Microfilming Vendor Contracts</td>
<td>Preauthorization Management Contracts</td>
</tr>
<tr>
<td>Optical Disc Conversion Contracts</td>
<td>Case Management Contracts</td>
</tr>
<tr>
<td></td>
<td>Third Party Administrator (TPA) Contracts</td>
</tr>
<tr>
<td></td>
<td>Wellness Promotion Contracts</td>
</tr>
</tbody>
</table>
**EXAMPLES OF ARRANGEMENTS THAT ARE NOT BUSINESS ASSOCIATE RELATIONSHIPS AND DO NOT REQUIRE BAAs/ADDENDUMS OR CONTRACT PROVISIONS**

<table>
<thead>
<tr>
<th>Banks Processing Credit Card Payments</th>
<th>Nursing Homes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blood Bank/Red Cross (Provider)</td>
<td>Organ Procurement Organizations</td>
</tr>
<tr>
<td>Clinics (Provider Relationships)</td>
<td>Pharmacy (Healthcare Provider/Treatment)</td>
</tr>
<tr>
<td>Courier Services Delivering Specimens</td>
<td>Providers (Involved in Care &amp; Treatment of Patient)</td>
</tr>
<tr>
<td>Device Manufacturers Require PHI to Produce</td>
<td>Quality Improvement Organization – Agent of CMS (MetaStar)</td>
</tr>
<tr>
<td>Pacemakers, Hearing Aids, Glasses, etc. (Treatment)</td>
<td>Rental Employee Agencies (No PHI Shared – Employees Need Privacy Training)</td>
</tr>
<tr>
<td>Cleaning/Janitorial Services</td>
<td>Repair Contractors (Maintenance, Copy Machine, Plumbing, Electricity, etc. – No PHI involved)</td>
</tr>
<tr>
<td>DME for Equipment for Treatment Purposes</td>
<td>School Health Nurses</td>
</tr>
<tr>
<td>Educational/School Programs (Student Privacy Education Required as Workforce Member)</td>
<td>Supply Services</td>
</tr>
<tr>
<td>Health Plans Contracting With Network Providers (Covered Entity to Covered Entity)</td>
<td>Support Services Agreements for Supplies/Tx Purposes</td>
</tr>
<tr>
<td>Health Plans for Purposes of Payment Hospitals</td>
<td>Tissue Banks</td>
</tr>
<tr>
<td>Housekeeping/Environmental Services (Incidental Exp.) Infusion Provider for Treatment</td>
<td>U.S. Post Office and Other Couriers</td>
</tr>
<tr>
<td>Law Enforcement Agencies</td>
<td>Volunteers (Board Members, Ethics Committee Members, IRB Members, etc.)</td>
</tr>
<tr>
<td>Members of an Affiliated Covered Entity</td>
<td></td>
</tr>
<tr>
<td>Members of Door County’s Organized Health Care Arrangement</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX 2: BUSINESS ASSOCIATE AGREEMENT CHECKLIST

An organization may serve as a BA to another CE or to another BA. CEs or BAs will ask the organization serving as a BA to review and sign a BAA. This Appendix contains a list of the minimum requirements for a BAA set forth under HIPAA’s Privacy and Security rules. This list may not contain all of the provisions necessary for an effective BAA and may not satisfy all of a CE’s or BA’s needs. CEs and BAs may want to include additional provisions (See Procedure 7 above). With respect to BAAs between a BA and another BA acting as a Subcontractor, the requirements in this Appendix apply in the same manner as such requirements apply to the agreement between a CE and BA.

This document is an Exhibit to the Business Associate Agreement Policy/Procedure document, but it, in itself, is not a valid BAA. For a BAA, Door County will utilize the HIPAA COW template BAA available at hipaacow.org.

<table>
<thead>
<tr>
<th>Date Received/Reviewed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received From (Department/Business Unit Leader):</td>
</tr>
<tr>
<td>Name &amp; Contact Information of BA:</td>
</tr>
<tr>
<td>General Description of Type of Service:</td>
</tr>
<tr>
<td>Other:</td>
</tr>
</tbody>
</table>

### PROVISIONS OF BUSINESS ASSOCIATE AGREEMENT

Establish the permitted and required uses and disclosures of PHI by the BA. The BAA may not authorize the BA to use or further disclose the information in a manner that would violate the requirements of the Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E), if done by the CE, except that:

A. The BAA may permit the BA to use PHI for the proper management and administration of the BA or to carry out the legal responsibilities of the BA.

B. The BAA may permit the BA to disclose PHI to third parties for the proper management and administration of the BA or to carry out the legal responsibilities of the BA if: (i) the disclosure is required by law; or (ii) the BA obtains reasonable assurances from the third party to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the third party and the third party notifies the BA of any instances of which it is aware in which the confidentiality of the PHI has been breached.

C. The BAA may permit the BA to provide data aggregation services relating to the health care operations of the CE.

(45 CFR § 164.504(e)(2)(i)(A)-(B) & 45 CFR § 164.504(e)(4)(i)-(ii))

Provide that the BA will not use or further disclose the information other than as permitted or required by the BAA or as required by law (45 CFR § 164.504(e)(2)(ii)(A) & 45 CFR § 164.103).

Provide that the BA will use appropriate safeguards and comply, where applicable, with the Security Rule (45 CFR Part 160 and Part 164, Subparts A and C) with respect to ePHI, to prevent use or disclosure of the information other than as provided for by the BAA (45 CFR § 164.504(e)(2)(ii)(B)).
<table>
<thead>
<tr>
<th>Provide that the BA will report to the CE any use or disclosure of the PHI not provided for by the BAA of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR § 164.410 (45 CFR § 164.504(e)(2)(ii)(C)).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide that the BA will report to the CE any security incident of which it becomes aware, including any breach of unsecured PHI as required by 45 CFR § 164.410 (45 CFR § 164.314(a)(2)(i)(C)).</td>
</tr>
<tr>
<td>Provide that the BA must, in accordance with 45 CFR §§ 164.502(e)(1) and 164.308(b)(2), enter into a BAA with any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA to ensure that the Subcontractor: (1) agrees to the same restrictions and conditions that apply to the BA with respect to the PHI; and (2) agrees to comply with the applicable requirements of the Security Rule. (45 CFR § 164.504(e)(2)(ii)(D) &amp; 45 CFR § 164.314(a)(2)(i)(B)).</td>
</tr>
<tr>
<td>Provide that the BA will make available PHI in accordance with 45 CFR § 164.524 (access of individuals to PHI) (45 CFR § 164.504(e)(2)(ii)(E)).</td>
</tr>
<tr>
<td>Provide that the BA will make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 CFR §164.526 (45 CFR § 164.504(e)(2)(ii)(F)).</td>
</tr>
<tr>
<td>Provide that the BA will make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528 (45 CFR § 164.504(e)(2)(ii)(G)).</td>
</tr>
<tr>
<td>Provide that, to the extent the BA is to carry out a CE’s obligation under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the CE in the performance of such obligation (45 CFR § 164.504(e)(2)(ii)(H)).</td>
</tr>
<tr>
<td>Provide that the CE will make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, the CE available to the Secretary for purposes of determining the CE’s compliance with the Privacy Rule (45 CFR § 164.504(e)(2)(ii)(I)).</td>
</tr>
<tr>
<td>Provide that the CE will at termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the BA on behalf of, the CE that the BA still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the BAA to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible (45 CFR § 164.504(e)(2)(ii)(J)).</td>
</tr>
<tr>
<td>Authorize termination of the BAA by the CE, if the CE determines that the BA has violated a material term of the BAA (45 CFR § 164.504(e)(2)(iii)).</td>
</tr>
</tbody>
</table>

Reviewed By/Date:
APPENDIX 3: BUSINESS ASSOCIATE QUESTIONNAIRE

Evaluating BA Satisfactory Assurances can be an investment to time and resources for distributing the questionnaires, meeting with BAs and analyzing the information that has been returned.

This document provides an organization with a list of questions surrounding key privacy and security topics in which to perform a review of additional satisfactory assurances for the entities you have selected as a BA. This is not an all-inclusive list, it is meant to provide a practical approach to verifying compliance.

This document should be completed by the BA prior to contracting with the BA to perform activities involving the creation, use, disclosure, transmission, storage, or destruction of PHI.

Balancing the Risk with Satisfactory Assurances

To determine which of the questions may be appropriate for your BA, consider the following and select questions that best provide a sense that compliance has been achieved:

• Which functions will the BA perform for or on CE’s behalf such as receiving, accessing, creating, modifying, storing, or transmitting data?

• What level of exposure to PHI would there be to unauthorized use or disclosure; increased risk of breach due to lack of security controls around data; potential security incident due to lack of encryption surrounding data in use, at rest and in motion?

• What risk of reputational harm or loss of business to the CE could be associated to the exposure of PHI?

• What risk of personal and financial impacts to members, patients or customers would there be if data was access or disclosed in an unauthorized manner?

• What level of commitment does the vendor have for compliance, what has been completed to date and what compliance controls are missing such as signed BAA, implemented and trained policies and procedures, annual review of policies and procedures, security training to new hires and existing staff annually, data security controls and the completion of the security risk analysis?

While selecting the questions that are most important for providing those satisfactory assurances, it will reduce risk to your organization due to the level of controls and compliance they have implemented.
**Business Associate Questionnaire**

What is the name and phone number of the organization’s privacy/security contact? 
______________

What is the name and phone number of one executive level leader? ________________

Approximately how many individuals as part of this contract will have access to Protected Health Information (PHI)? ____________

What was the date of the organization’s last HIPAA Security Risk Assessment? ____________

<table>
<thead>
<tr>
<th>YES</th>
<th>NO</th>
<th>IN PROGRESS</th>
<th>SECURITY TOPICS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TRAINING</strong> = Are workforce members trained on an annual basis whom to call if PHI is lost or stolen or another type of incident happens that may have resulted in an unauthorized use or disclosure of PHI?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>CONFIDENTIALITY AGREEMENT</strong> = Do you require anyone having access to PHI to sign a confidentiality agreement that includes reference to HIPAA Privacy and Security responsibilities?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>MINIMUM NECESSARY</strong> = Do you have a policy for workforce members to only use, access and request PHI that is necessary in order to perform the duties of their job?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>PASSWORDS</strong> = Do you have procedures for creating, changing, and safeguarding passwords?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>E-MAIL</strong> = Do you have a policy not to e-mail PHI and/or not to e-mail unencrypted PHI?</td>
</tr>
</tbody>
</table>

**Review note**

Training less than annually may indicate policies and procedures are outdated; staff is less informed and processes for handling an incident may not be done appropriately.

Indicator that the organization is holding employees accountable for their actions by informing them of their responsibilities for handling data.

An organization should review the types of information they are requesting or disclosing and be familiar with minimum necessary data required to complete the required function or activity.

Passwords that are not forced to change are more susceptible to hacking opportunities. Strong password policies should be in place to prevent automated systems from accessing the systems.
<table>
<thead>
<tr>
<th><strong>Review note</strong></th>
<th><strong>Unencrypted emails for external transmission can expose information to a breach without the ability to track.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM ACCESS AND TERMINATION</strong> = Do you have a policy and procedure on granting access and terminating access to systems that contain PHI?</td>
<td></td>
</tr>
<tr>
<td><strong>Review note</strong></td>
<td><strong>Documented procedures ensure there is a tracking mechanism for all access that has been granted allowing proper termination of access when it is needed. Undocumented procedures may leave some web-based systems accessible to terminated employees.</strong></td>
</tr>
<tr>
<td><strong>ENCRYPTION</strong> = Do you encrypt your laptops and any other portable media (flash/thumb drives) that contain PHI?</td>
<td></td>
</tr>
<tr>
<td><strong>Review note</strong></td>
<td><strong>Portable devices are one of the leading causes of major breaches, encrypting these devices offers a level of security in the event there is a lost or stolen device.</strong></td>
</tr>
<tr>
<td><strong>ANTI-VIRUS AND ANTI-MALWARE</strong> = Do you have anti-virus and anti-malware procedures for guarding against and detecting malicious software (virus, Trojan horse, worm, etc.) for workstations and laptops that is current and updated regularly?</td>
<td></td>
</tr>
<tr>
<td><strong>Review note</strong></td>
<td><strong>New viruses and malware are released every day, automated anti-virus and anti-malware software protects systems against these attacks.</strong></td>
</tr>
<tr>
<td><strong>PATCHING</strong> – Do you patch systems regularly?</td>
<td></td>
</tr>
<tr>
<td><strong>Review note</strong></td>
<td><strong>Applying patches and updates manually is effective as long as it is done on a reasonable routine basis.</strong></td>
</tr>
<tr>
<td><strong>AUTOMATIC LOG-OFF</strong> = Are automatic logoffs activated for all systems containing or that transmit PHI?</td>
<td></td>
</tr>
<tr>
<td><strong>Review note</strong></td>
<td><strong>Unauthorized access can be internal or external, systems that are used for creating, accessing, storing, modifying or transmitting data should not be left unattended for periods of time that extend beyond 15 or 20 minutes (reasonable). Automated log-offs should boot the person from the screen they are working to require them to re-log onto the system. It should not freeze the screen on the data in use at the time the account locked out.</strong></td>
</tr>
<tr>
<td><strong>REUSE AND DISPOSAL OF MEDIA</strong> = Have you implemented policies and procedures to remove/destroy PHI on hardware or electronic media you are no longer using?</td>
<td></td>
</tr>
</tbody>
</table>
Review note | Hardware, electronic media or portable devices need to be properly erased prior to re-use to prevent unauthorized access or disclosures. Disposal of equipment or media must ensure the data is unreadable, unusable.
---|---
**SHREDDING** = Do you have shredding procedures for hard copy PHI?
---|---
Review note | Information shredded according to the NIST disposal practices would be considered “secured PHI”. Information shredded in a manner to leave the material unidentifiable, unusable, unreadable may still be compliant but it would not be considered secured PHI.
---|---
**BACK-UP** = Is data at risk for non-recovery given the current back-up procedures?
---|---
Review Note | **PHYSICAL SECURITY** = Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft?
---|---
Review note | Implementing measures to protect the physical security of data including the facilities, server rooms, workstations, equipment, and back-up locations will minimize the risk for unauthorized access.
---|---
**HOME OFFICE** = Do you have workforce members who work at home? If yes, do you have additional security requirements for their home office environment?
---|---
Review note | Do all Home Office workers have strong security enabled networks at home?
---|---
Review note | **INVESTIGATION** = Do you have policies and procedures addressing how security incidents and potential breaches will be investigated?
---|---
Review note | Understanding the assessment process the organization will go through to determine what happened, how it happened, when it happened and what the short and long-term effects of the activity causing the breach to occur are. The organization should have a documented policy for conducting this breach assessment which should map to the required notification requirements.
---|---
**BREACH RISK ASSESSMENT** = Do you use a risk assessment tool to determine if there is more than a low probability the information has been compromised resulting in a breach?
---|---
Review note | The regulations provide an assessment for use, is the organization using it?
<table>
<thead>
<tr>
<th>BAA = Do you obtain Subcontractor Business Associate Agreements from subcontractors that have access to PHI?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review note</td>
</tr>
</tbody>
</table>
POLICY:
Door County will control access to and within facilities as part of the Door County’s efforts to safeguard the confidentiality, integrity, and availability of Protected Health Information (PHI) and electronic Protected Health Information (ePHI). This involves striking a balance between appropriately limiting physical access, while ensuring that properly authorized access is allowed.

PROCEDURE:

1. **Identification of Persons at Door County Facilities**
   1.1. Employees, appointed officials, and elected officials (“persons”) wear identification badges at all times while at any Door County facilities.
   1.2. Persons are required to return their Door County identification badge to the Human Resources Department or designee on their last day of employment or expiration of the term for which s/he was appointed or elected.
   1.3. Visitors (e.g., vendors and contractors) check in with the Department Head or designee.

2. **Security of Restricted Areas**
   2.1. Restricted areas and facilities are (if and to the extent feasible) locked and alarmed when unattended.
   2.2. Only authorized employees, appointed officials and elected officials (“persons”) receive keys/key codes to access restricted areas (as determined by the Security Official, or designee, through Facility requests).
   2.3. Persons are required to return the key(s) to the Human Resources Department or designee on their last day of employment or expiration of the term for which s/he was appointed or elected. Key codes will be deactivated.
   2.4. Persons must report a lost and/or stolen key(s) to the Security Official, or designee,
   2.5. The Security Official, or designee, facilitates the changing of the lock(s) and key pad codes within 24 hours of a key being reported lost/stolen.

3. **Persons Allowed in Restricted Areas:**
   3.1. Employees, appointed officials, and elected officials (“persons”) as approved based on their role or function and as needed to perform their duties.
   3.2. Persons with an authorized escort into and out of the areas.
   3.3. Family members and friends briefly visiting persons with an authorized escort.
   3.4. Vendors with an authorized escort into and out of the areas.
   3.5. Vendors on a long-term contract, once acclimated to the areas, without an escort.

4. **Persons Allowed in Unrestricted Areas:**
   4.1. Employees, appointed officials, and elected officials (“persons”)
   4.2. Vendors
4.3. Persons’ family members and friends

4.4. Visitors

5. Enforcement

5.1. Escort violators out of restricted areas immediately and escort them to the area they are trying to get to.

5.2. All employees, appointed officials, and elected officials (“persons”) are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to a facility and/or areas containing information systems that store and/or transmit ePHI to the Security Official, or designee.

5.3. Persons in violation of this policy are subject to sanction or disciplinary action (up to and including termination).

5.4. Vendors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Door County.

6. Workstation Security

6.1. Workstations may only be accessed and utilized by authorized employees, appointed officials, and elected officials (“persons”) wearing appropriate identification to complete assigned responsibilities. Third parties may be authorized by the Security Official to access systems/applications on an as needed basis.

6.2. All persons are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.

6.3. All Door County servers and network hardware are maintained in secured, locked area/room. Access to these rooms is limited to authorized persons as required to perform duties (e.g., to maintain these rooms and/or the equipment within these rooms). Access by anyone else is granted only by approval from the Security Official and only with an escort by an authorized person.

6.4. Permanent Workstations (i.e. desktop computer, printers, and monitors) may only be moved by authorized persons.

6.5. All wiring associated with a workstation may only be installed, fixed, upgraded, or changed by the Security Official, or designee.

7. Documentation

7.1. The Security Official will maintain documentation on the Inventory Asset List of physical security controls in place at each location. i.e., alarm systems, locked file cabinets, key/keypad panels, etc.

DEFINITIONS

1. **Restricted Area**: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored or utilized at any time. These areas include, but are not limited to the following examples:

   1.1. Health information management/medical record departments,
   1.2. Check-in desks/stations,
   1.3. Patient Care areas (e.g., stations/desks, hallways, rooms and other designated patient care areas),
   1.4. Mailrooms,
   1.5. Offices,
   1.6. Cubicles,
   1.7. Storage closets and cabinets (including medication storage areas),
   1.8. Information Services equipment rooms,
   1.9. Business Office offices,
1.10. Human Resources offices, and
1.11. Administration offices.

2. **Unrestricted Area**: those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized there on a regular basis. These areas include the following:
   2.1. Break / Lunch rooms,
   2.2. Conference rooms,
   2.3. Building parking lots,
   2.4. Building entry ways,
   2.5. Main hallways, and
   2.6. Restrooms.
   2.7. Other public areas.

**REFERENCES:**

*Regulatory Source:*

45 CFR §164.310(a) HIPAA Security Rule Facility Access Controls
45 CFR §164.310(a)(2)(iii) HIPAA Security Rule Access Control & Validation Procedures
HIPAA COW Facility Access Policy, Version 7, 3/31/2010

**POLICY OWNER:** Security Official

**APPROVED BY:** Door County Administrative Committee (December 11, 2018)
Title: HIPAA Facility Maintenance and Repairs
Policy Type: HIPAA Security
Policy Number: 10
Entities Affected: County of Door
Effective Date: March 1, 2018

POLICY:
Door County will document maintenance and repairs to the physical security of the facilities.

PROCEDURE:
1. Before making any repair and change that may impact the security of the facility, the plans are reviewed and approved by the Security Official or designee.
2. The Security Official or designee is responsible to work with the facility to ensure, whenever possible, repairs and change plans:
   2.1 Improve security measures.
   2.2 When making significant changes, an evaluation is done on whether it is feasible to add additional security controls, and these are added to the plans.
   2.3 Do not have the ability to pose a new security risk, or reduce current security controls.
3. The Security Official or designee documents all repairs and changes made, for example to locks, including what was done, reasons for it, who completed it, and start and end dates.
4. The Security Official or designee will maintain a maintenance log that includes regularly scheduled or anticipated activity for regulatory codes, equipment upkeep, and safety. This includes, but is not limited to, structural security, fire safety surveys, protections for any equipment that contains ePHI and security equipment testing. Documentation of maintenance requested and paid by Door County includes date, reason for maintenance, and authorizing individual.
5. All documentation is maintained by the Security Official or designee for six years.

REFERENCES:
Regulatory Source:
45 CFR §164.310(a)(2)(iv) HIPAA Security Rule Maintenance Records
HIPAA COW Facility Repairs and Maintenance Policy, Version 2, 4/19/2005

POLICY OWNER: Security Official
APPROVED BY: Door County Administrative Committee (February 20, 2018)
<table>
<thead>
<tr>
<th>Title:</th>
<th>Re-Use and Disposal of Electronic Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Type:</td>
<td>HIPAA Security</td>
</tr>
<tr>
<td>Policy Number:</td>
<td>11</td>
</tr>
<tr>
<td>Entities Affected:</td>
<td>County of Door</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>June 1, 2018</td>
</tr>
<tr>
<td>Revision Dates:</td>
<td></td>
</tr>
</tbody>
</table>

**POLICY:**

Door County will ensure the privacy and security of sensitive and electronic protected health information (ePHI) in the reuse and destruction/disposal of electronic media.

**PROCEDURE:**

1. Technology Services will oversee and document the removal/sanitization of sensitive electronic media before the media are made available for re-use.

2. 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), Technology Services removes all sensitive data and/or makes it inaccessible, cleaned, or scrubbed through one of the following methods:
   2.1. Overwrite the data (for example, through software utilities).
   2.2. Degauss the media; or
   2.3. Reformat it so that files are not accessible to the new user(s)

3. Technology Services will oversee and document the final disposition/disposal of all electronic media on which sensitive data has been stored.

4. Destruction/Disposal/Sanitization documentation may be done on Door County’s Certificate of Destruction form which includes the following information:
   4.1. Date of destruction/disposal/sanitization;
   4.2. Method of destruction/disposal/sanitization;
   4.3. Description of the destroyed/disposed/sanitized record series or medium;
   4.4. Inclusive dates covered;
   4.5. A statement that the sensitive information was destroyed/disposed/sanitized in the normal course of business; and
   4.6. The signatures of the individuals carrying out the destruction/disposal/sanitization.

5. Technology Services will maintain an inventory asset list, including a record of the destruction method used for disposed of or reused of electronic media.

6. Examples of methods used for the destruction/disposal/sanitization may include:
<table>
<thead>
<tr>
<th>Medium</th>
<th>Method Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audiotapes</td>
<td>• Recycle (tape over), Degauss or pulverize.</td>
</tr>
</tbody>
</table>
| Electronic Data/ Hard Disk Drives including drives found in servers, workstations, printers, and copiers | • Destroy data permanently and irreversibly through a DoD wipe, physical destruction (pulverize, shred, disintegrate, incinerate), Degaussing of it, or hard drive erasure software.  
  • Methods of reuse: overwrite data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten. |
| Electronic Data/ Removable Media or devices including USB drives, SD cards, CDs, tapes, and cartridges | • Overwrite data with a series of characters or reformat it (destroying everything on it). Total data destruction does not occur until the data has been overwritten.  
  • Magnetic Degaussing that leaves the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic Degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable.  
  • Shredding or pulverization is done for the final disposition of any removable Media when it is no longer usable. |
| Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices | • Activate the Software on these devices that remotely wipes data from them.  
  • When a handheld device is no longer reusable it is then totally destroyed by recycling or by trash compacting. |
| Optical Media                               | • Optical disks cannot be altered or reused, making pulverization or cutting an appropriate means of destruction/disposal. |
| Microfilm/ Microfiche and X-rays            | • Recycle through a contracted BA or pulverize.                            |
| PHI Labeled Devices, Containers, Equipment, Etc. | • Reasonable steps should be taken to destroy or de-identify any sensitive data/PHI information prior to disposal of this medium. Remove labels or incineration of the medium; or  
  • Obliterate the information (make it unreadable) with a heavy permanent marker pen.  
  • Ribbons used to print labels may contain sensitive data/PHI and are shredded or incinerated. |
| Paper Records                               | • Paper records are destroyed/disposed of in a manner that leaves no possibility for reconstruction of the information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing. If shredded, use cross cut shredders which produce particles that are 1 x 5 millimeters or smaller in size. |
| Videotapes                                  | • Recycle (tape over) or pulverize.                                        |

**REFERENCES:**

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 §164.310(d)(2)(iii) HIPAA Security Rule Accountability  
HIPAA COW Device, Media, and Paper Record Sanitization for Disposal or Reuse Policy, 10/8/2012

**POLICY OWNER:** Security Official  

**APPROVED BY:** Door County Administrative Committee (May 15, 2018)
TITLE: Technical Access Controls: Transmission Security, Encryption, and Integrity Controls

POLICY TYPE: HIPAA Security

POLICY NUMBER: 12

ENTITIES AFFECTED: County of Door

EFFECTIVE DATE: June 1, 2018

Revision Dates:

POLICY:
Door County will implement mechanisms to securely encrypt and decrypt sensitive/ePHI at rest and in transit, whenever possible and deemed appropriate to help protect such data.

PROCEDURE:

Encryption and Other Mechanisms Used to Secure sensitive/ePHI at Rest and In Transit

1. Door County makes every effort possible to encrypt sensitive/ePHI at rest and in transit, to prevent unauthorized access, alteration, and destruction.

2. Technology Services along with appropriate officials/representatives evaluates risks to determine the need and ability to encrypt sensitive/ePHI, as well as the type of encryption to use. 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 the data, loss of reputation, as well as other factors and/or negative impacts that may happen based on the decision.

2.1. If it is determined that the data will be encrypted:

2.1.1. Door County makes every effort to select encryption products that are certified to meet the highest possible standards.(e.g., FIPS 140-2 Standard). This helps ensure that it will meet any criteria specified by Federal law, either now or in the foreseeable future, be more than sufficient to pass an audit, and eliminate the need to provide breach notifications.

2.1.2. Strong passwords of at least 8 characters are used when creating encryption passwords (as required in the System Access Policy). If weak passwords are used such as a pin they must still remain 8 characters in length and have other methods used to prevent attacks on the password.

2.1.3. Users do not share encryption user names and passwords or leave them so someone else may see/find them (refer to the System Access Policy).

2.1.4. Encryption Keys are secured and stored so that only the minimum necessary individuals with the authority to access encrypted servers and backups to maintain them have access to them.

3. Workstations (computers, laptops, USB/Flash Drives, CDs, Smart phones, etc.)

3.1. Removable media should not be used to store sensitive/ePHI data

3.2. Door County takes steps to encrypt sensitive/ePHI data stored on Workstations and/or encrypt the devices themselves.

4. Backups

4.1. Backups that contain sensitive/ePHI or the data within the backups is/are encrypted.

5. Emails

5.1. Standard emails are inherently not a secure method of communication and can, therefore, be intercepted by unauthorized individuals.
5.2. Workforce members must follow Door County’s E-mailing PHI policy and procedures to properly encrypt sensitive/ePHI data.

5.3. An encryption appliance is used as a final fail-safe to monitor for and encrypt sensitive/ePHI information through the e-mail system.

6. Texts

6.1. Texting is an unsecured method of communication and can, therefore, be intercepted by unauthorized individuals.

6.2. Door County does not have a means to encrypt texts, Door County’s sensitive/ePHI may not be texted at any time from any device, whether or not the texting device is owned by the Door County.

7. Network Transmissions (of sensitive/ePHI to/from other entities/sites as well as internally)

7.1. Sensitive/ePHI is transmitted only when allowed by this policy and the organization’s Release of Information Policies.

7.2. One of the following methods is used for external network transmissions which are set up and monitored by the Technology Services. Exceptions are reviewed, approved, and authorized by the Technology Services Department.

7.2.1. Protected communication paths should be used, these include:
   7.2.1.1. Secure Shell (SSH)
   7.2.1.2. Secure File Transfer Protocol (SFTP);
   7.2.1.3. Secured Socket Layers (SSL) or Tunnel Layer Security (TLS)
   7.2.1.4. HTTPS.

7.2.2. Remote access through:
   7.2.2.1. The Virtual Private Network (VPN) (private point-to-point network).
   7.2.2.2. Citrix, through the Citrix Access Gateway product.

7.3. Only Workstations (including portable devices) authorized by Technology Services are allowed on the Door County’s network.

7.4. Unused data jacks are disabled to prevent non-organization devices to connect to the network without the organization’s knowledge.

8. Wireless Access Points

8.1. WPA2 is in place for all non-public wireless access points. A strong password is utilized to access them (refer to the System Access Policy for minimum password requirements). This password should not be shared and Technology Services is to place on devices whenever possible.

8.2. Only Workstations authorized by Technology Services are allowed on the organization’s wireless network.

8.3. A separate public wireless network is available for visitors’ use.

Documentation

1. Technology Services documents all decisions and approvals made related to this policy and its corresponding procedures.

2. Technology Services maintains all documentation for six years from the date of creation or date it was last in effect, whichever is later.

REFERENCES:

45 C.F.R. §164.312(e)(1) HIPAA Security Rule Transmission Security
45 C.F.R. §164.312(a)(2)(iv) HIPAA Security Rule Encryption and Decryption
45 C.F.R. §164.312(e)(2)(ii) HIPAA Security Rule Encryption
45 C.F.R. §164.312(c)(1) HIPAA Security Rule Integrity
45 C.F.R. §164.312(c)(2) HIPAA Security Rule Mechanism to Authenticate Electronic PHI
45 C.F.R. §164.312(e)(2)(i) HIPAA Security Rule Integrity Controls
45 C.F.R. §164.312(e)(1) HIPAA Security Rule Transmission Security
HIPAA COW Encryption Whitepaper, 2010

POLICY OWNER: Security Official

APPROVED BY: Door County Administrative Committee (May 15, 2018)
To: Administrative Committee  
From: Kelly Hendee, Human Resources Director  
Date: May 12, 2021  
Re: Human Resources Areas of responsibility  

According to Society for Human Resource Management, HR Department Benchmarks rule-of-thumb ratio is 1.4 full-time HR staff per 100 employees. The County has approximately 475 employee’s which stem from full time to part time benefited positions as well as a number of reserves, LTE’s and interns.

Human Resources currently has three (3) employees working full time, which falls short of the industry standard. With todays ever changing landscape of employment law, and hiring challenges, the pressure to add staff is high. Some examples of how low staffing impacts the organization is: one employee is out on FMLA (Family Medical Leave) for ¼ of the year – other staff wanting to take off leave the department staffed with one person and often times with multiple interviews going on this will leave no one in HR.

Another example is burn out, working 45+ hours (most of the time 50), on an ongoing basis, year after year, no lunches, in early – out late, is not sustainable.

And most importantly we are not serving our current employee base as we could and should for retention purposes and to create a culture that reflects the Employer of choice which ultimately retains staff.

The scope of Door County Human Resources refers to all the activities that come under the banner of HRM (Human Resources Management). The activities are as follows

1. **Human resources planning:** – Human resource planning is a process by which the County identifies the number of jobs vacant, whether the county has excess staff or shortage of staff and to deal with this excess or shortage.

2. **Job analysis design:** – Another important area of HRM is job analysis. Job analysis gives a detailed explanation about each and every job in the county. Based on this job analysis the county uses this to prepare advertisements.

3. **Recruitment and selection:** – Based on information collected from job analysis the HR department prepares advertisements and publishes notifications for openings. A number of applications are received after the advertisement is published, interviews are conducted and the right employee is selected thus recruitment and selection are yet another important area of HRM.
4. **Orientation and onboarding:** – Once the employees have been selected an onboarding or orientation program is conducted. The employees are informed about County policy and organization. They are told about the organizational culture and values and work ethics and introduced to the other employees thru new employee luncheons.

5. **Training and development:** – Every employee will participate in onboarding training which helps them better perform on the job and understand County culture. Training programs are also conducted for existing staff, called refresher training. Training and development is one area where the county will have to look at spending to succession plan.

6. **Performance appraisal:** – Once the employee has put in one (1) year of service, a performance appraisal is conducted i.e. HR processes the evaluations, which are kept in their respective personnel files to serve as documentation for future promotions, incentives, and increments in salary.

7. **Compensation planning:** – There are various rules regarding compensation and other benefits. It is the job of the HR department to look into compensation planning.

8. **Benefits:** - it is the responsibility of HR to oversee the benefits provided to employees and ensure they remain competitive and follow areas of compliance.

9. **Policy and Procedure:** - It is the responsibility of HR to oversee, update, implement policy and make recommendations to the County Board for policy and policy review.

10. **Motivation, wellness, health and safety:** – Motivation becomes important to sustain the number of employees in the organization. It is the job of the HR department to look into the different methods of motivation. Apart from this certain health and safety regulations have to be followed for the benefits of the employees.

11. **Industrial relations:** – Another important area of HRM is maintaining co-ordinal relations with the union members. This will help the organization to prevent poor relations and ensure smooth working in the county.
perspectives

The Numbers Tell the Story of Our Labor Shortage

by STEPHEN R. GRUTZMACHER
steven@pulise.com

One of the favorite parts of my job at Peninsula Publishing & Distribution is meeting with, talking with and - occasionally - debating with business owners, community leaders and others throughout the Door peninsula. I learn all manner of things during these conversations, and more often than not, the things I learn I share with my Peninsula Pulse co-workers, which often leads to stories that appear in the paper.

Sometimes, however, I become frustrated by these conversations and, eventually, I feel compelled to sit down and write a story. Such is the case with the topic of employment on the peninsula.

As even the most casual observer must realize, the Door peninsula is in the midst of a huge worker shortage. What is less clear to people is the extent of the problem and the reasons for the shortage. Although the tourism season requires a significant increase in workers, Debra Fitzgerald's story in the April 9-16 issue of the Pulse documented the shortage of manufacturing workers and the struggles of that industry to find those workers. So the problem goes beyond seasonal jobs.

Unfortunately, some of the frustrated employers I have talked with during recent months have pointed to the stimulus checks and the potential $300 extra per week in unemployment that people can receive. They then leap to the assumption that individuals are not applying for jobs because they are being "paid to stay home." Are there individuals out there for whom this assumption is true? It would be disingenuous to assert that there aren't some. But the reasons for the employment problem are far greater and have been with us for decades.

- Look through the help-wanted ads in recent issues of the Pulse, and you will see pages of ads seeking machinists, HVAC installers and medical workers alongside the ads for housekeepers, servers, bartenders and cooks.

The lack of international student workers last year and the uncertainty surrounding those workers this year certainly play a role in filling many of these positions, but the shortage goes far beyond the scope of what these workers can fill.

For years I have said and written that Door County's single greatest asset and single greatest liability are the same: It's a peninsula. Unlike many other vacation destinations, we have no surrounding areas from which to draw workers. And the reality is that the county's population has been stagnant, hovering between 27,000 and 28,000 full-time residents for decades.

The other reality is that we are aging. Although baby boomers aging out of the workforce in this country has been a well-documented story in recent years, the challenge of an aging workforce has been with Door County since the turn of the century. I first began writing about this in 2001, but I recently revisited some of my old sources, particularly the United States Census website, to see where things stand today.

The "Door County Estimate Population 2019" shows the estimated population of Door County in 2019, broken down into five-year age brackets. Here are three quick things that I observed from the data:

- The total population between the ages of 20 and 59 - the prime workforce age range - is just 12,078, or 44% of the total population. Some in this group have legitimate reasons for not participating in the workforce. We have some youths ages 15-19 and many adults older than 60 who participate in the workforce, at least part time, but the 20-59 age group remains the prime workforce.
- Of that 12,078, the total number of people who are 50-59 is 4,226, or 35% of the prime workforce age group. In nine years, this entire group will be 60-69.
- The age group from birth to 19 totals just 4,850, which is 11.3% less than the 5,468 residents ages 60-69. And, as we know, a significant number of our young people will move off the peninsula when they become adults. So we are not replacing those aging out of the workforce with an equal number joining the workforce.

Perhaps the easiest way to understand the real cause of the worker shortage in Door County is to look at the table titled "2018 Employment by Industry Door Co.," which is a portion of a larger table posted on the Wisconsin Department of Workforce Development's website. Again, feel free to scan through this information at your leisure, but for the purposes of this column, look at the last listing: "All Industries 13,728." Then compare that number to the estimated number in the "prime workforce age group" that I outlined above: 12,078.

That disparity, folks, is the crux of our current employment crisis: There are simply not enough residents living on our peninsula to fill the jobs we have available.

Are there some people who are sitting back, collecting unemployment with the additional $300 per week, and therefore not choosing to work, as some employers claim? Probably, but their numbers are insignificant compared to the real problem.

In order to fill the multitude of job openings, we need a larger pool of workers. In order to enlarge our pool of workers, they need to live in Door County. But this is not an easy fix. Unfortunately, the challenges to people relocating to our peninsula include housing, child care, the low wage scale for most industries in Door County, and our high cost of living.

The reality is that this will be a difficult season for Door County. Businesses will be short staffed. Seasonal fatigue will set in far earlier than usual for owners and employees. International student workers will help next year if all goes well, but we are going to need to actively address our employee shortage by focusing on the impediments that keep workforce-eligible workers from moving here - starting now.

For example, I don't particularly like so far as giving him a fake award at a saved taxpayers lots of money. It's a 2019 saloon.
**Request to Refill Position**

**DEPT. HEAD TO COMPLETE:**

<table>
<thead>
<tr>
<th>Department</th>
<th>Sheriff’s Office</th>
<th>Position Title: Patrol Deputy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position Status:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Will be vacant</td>
<td></td>
<td>Date Vacant: July 2, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hours per week: 1947 Hours Annually</td>
</tr>
<tr>
<td>Reason for Vacancy:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Retirement</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transfer: why is the new position more attractive to employee than current one?

Name of Current / Most Recent Incumbent: Timothy J Fuerst

☑️ I have invited the Chair of my Oversight Committee to participate in the interview process

Reviewed, updated, and submitted to Human Resources:
- ☑️ Job Analysis Questionnaire *(not to be included in the agenda packet)*
- ☑️ Job Description

Completed by: Sheriff Tammy A. Sternard Date 05-03-2021

**Financial Information:**

<table>
<thead>
<tr>
<th>Salary Range:</th>
<th>$27.14 - $32.27 Hourly</th>
<th>Is the Position Budgeted:</th>
<th>☑️ Yes</th>
<th>☐ No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funding Source:</td>
<td>☑️ Levy % 100</td>
<td>☐ Grant Funded</td>
<td>%</td>
<td>☐ Other</td>
</tr>
<tr>
<td>☑️ Fiscal Impact, from Finance Department, completed and attached</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**HR TO COMPLETE:**

<table>
<thead>
<tr>
<th>EEO Protected Services</th>
<th>FLSA Status Non - exempt</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️ Human Resources has performed a position review?</td>
<td>KH <em>(HR initial)</em> 5/5/2021 Date</td>
</tr>
<tr>
<td>☑️ The Job Description has been updated and signed?</td>
<td>KH <em>(HR initial)</em> 5/5/2021 Date</td>
</tr>
</tbody>
</table>

**Approvals:**

County Administrator ____________________________ Date 5/6/2021

Administrative Committee Chair ____________________________ Date ____________________________
General Summary

Under the general direction of the Sheriff, Chief Deputy, Professional Standard Captain and Field Service Lieutenant. The Patrol Shift Sergeant is the direct supervisor. This position is responsible for enforcing all state, county, and federal laws and regulations; investigates criminal activities; assists citizens; and investigates accidents; makes arrests; does criminal & process serving; completes routine public relations activities. Responsible for providing truthful and accurate written and verbal communications. Regular attendance and punctuality along with being prepared to commence work at designated work locations, on the assigned or scheduled days and hours is expected.

Duties and Responsibilities

**Essential Job Functions**

1. Works on assigned shifts in vehicle performing security patrols, traffic control, investigation and first aid at accidents, detection, investigation and arrest of persons involved in crimes or misconduct.
2. Maintains normal availability by radio and telephone, with supervisory personnel to coordinate activities, for consultation on major cases and provides general information about department activities.
3. Undertakes community-oriented police work, and assists citizens with such matters as locked or stalled vehicles, crime prevention, traffic safety, etc.
4. PatROLS streets/routes, parks, commercial and residential areas to preserve the peace and enforce the law, control vehicular traffic, prevent or detect and investigate misconduct involving misdemeanors, felonies and other law violations' and to otherwise serve and protect.
5. Responds to emergency radio calls and investigates accidents, robberies, civil disturbances, domestic disputes, fights, drunkenness, missing children, prowlers, abuse of drugs, etc. Takes appropriate law enforcement action.
7. Conducts follow-up investigations of criminal law violations occurring within lawful jurisdiction during assigned shift. Seeks out and questions victim(s), witnesses and suspects. Develops leads and tips. Searches scene of a crime for clues. Analyzes and evaluates evidence by compiling information regarding these crimes, preparing cases or filing of charges and arrests offenders. Prepares cases for giving testimony and testifies in court proceedings.
8. Prepares a variety of reports and records including reports of investigation, field interrogation report, alcohol reports, influence reports, breathalyzer check list, bad check form, vehicle impoundment form, traffic hazard report, etc.
9. Receive and make service of civil process.

General Job Functions
1. Works an assigned shift using own judgment in deciding course of action being expected to handle difficult and emergency situations without assistance.
2. Coordinates activities with other officers/deputies or other departments as needed, exchanges information with officers/deputies in other law enforcement agencies, and obtains advice from the District Attorney's Office and Corporation Counsel Office regarding cases, policies and procedures, as needed and assigned.
3. Carries out duties in conformance with Federal, State, County, and City laws, ordinances and departmental policies and procedures.

Requirements

Training and Experience
1. High School diploma or equivalent.
2. Must possess a minimum of sixty (60) college credits from an accredited college or university in police science, criminal justice, or related field.
3. Wisconsin Law enforcement certified, certifiable or within 6 months of graduation from an accredited criminal justice related program.
4. Successful completion of Deputy Sheriff Patrol – Field Training Officer (FTO) training and evaluation program.

Knowledge, Skills and Abilities Required
1. Knowledge of laws, regulations, ordinances and departmental policies and procedures which impact duties on patrol.
2. Knowledge of personal self-defense.
3. Ability to use tact and discretion to optimize safety and control.
4. Ability to react quickly, both mentally and physically, to any situation.
5. Knowledge and ability to use a computer and current software programs.
6. Ability to prepare accurate reports.
7. Ability to operate: equipped cruiser: radio, radar, handgun and other weapons as required, baton, handcuffs, computer, first aid equipment, copy machine, fax machine, camera, PBT, Taser, and other related equipment to the patrol position.
8. Ability to use tact and courtesy in maintaining an effective working relationship with department employees, county supervisors, county officials, and general public.
9. Ability to read, comprehend, and communicate, both verbally and in writing.

Physical and Work Conditions
The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is frequently required to sit and talk or hear. The employee is occasionally required to stand; walk; use hands to finger, handle, or feel objects, tools, or
controls; reach with hands and arms; climb or balance; stoop, kneel, crouch, or crawl; and taste or smell.

The employee must occasionally lift and/or move up to 60 pounds. Specific vision abilities required by this job include close vision, distance vision, color vision, peripheral vision, depth perception, and the ability to adjust focus.

Work conditions vary by shift. Few tasks require heavy lifting, pushing, pulling, or carrying heavy loads. Flexibility is important because of the need to enter and exit vehicles frequently, inspect buildings, climb over and around obstacles, suddenly move out of the way of dangers, etc. Mental alertness is very important because of the need to make fine discriminations and decisions concerning subtle cues of impending danger or to discover inconsistencies in witnesses or suspects' testimonies, etc.

In an effort to provide for continuity of County government and to cope with the problems of the emergency, you may be required to work during a proclaimed state of emergency, consistent with Sec. 323.14, Wis. Stats. and County emergency management plans and programs.

The above is intended to describe the general content of the requirements for the performance of this job. It is not to be construed as an exhaustive statement of duties, responsibilities or requirements. They may be subject to change at any time due to reasonable accommodation or other reasons.

The above statements are intended to describe the general nature and level of work being performed by people assigned to this position. They are not intended to be an exhaustive list of responsibilities, duties and skills required of personnel so classified. This description is not intended to limit or modify the right of any supervisor to assign, direct and control the work of employees under supervision. Door County retains and reserves any or all rights to change, modify, amend, add to or delete from the section of this document as it deems, in its judgment, to be proper.

Approvals:

Tammy Steward, Sheriff 3-3-2021 3/3/2021
Kelly A. Hendee, Human Resources Director Date
REQUEST FOR FISCAL IMPACT INFORMATION

RECLASSIFICATION

<table>
<thead>
<tr>
<th>Position Title</th>
<th>Patrol Deputy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date</td>
<td>6 Mo</td>
</tr>
<tr>
<td>Department</td>
<td>Sub Dept</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Patrol Deputy-Level F-Starting Point</th>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
<th>TOTAL SALARY and Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00 @ $27.14</td>
<td>53,065</td>
<td>37,818</td>
<td>90,883</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget Patrol Deputy-Level F-Step 7</th>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
<th>TOTAL SALARY and Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00 @ $32.27</td>
<td>63,096</td>
<td>40,090</td>
<td>103,186</td>
</tr>
</tbody>
</table>

Total Salary and Benefit Decrease (12,303)

<table>
<thead>
<tr>
<th>Patrol Deputy-Level F-Step 7</th>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00 @ $32.27</td>
<td>63,096</td>
<td>40,090</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget Patrol Deputy-Level F-Step 7</th>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00 @ $32.27</td>
<td>63,096</td>
<td>40,090</td>
</tr>
</tbody>
</table>

Total Salary and Benefit Increase 103,186

Dept Head Signature
Finance Director

Date 5/13/2021

Disclaimer: This Fiscal Impact does not include Step 1 $27.82, Step 2 $28.52, Step 3 $29.23, Step 4 $29.96, Step 5 $30.71 and Step 6 $31.48.

This Fiscal Impact is an example illustration of what the costs would be for this position/position change. It is based on estimates and assumptions provided by the Human Resources Department and/or the department in which this position works. Because these estimates and assumptions may change, or may be different than the actual circumstances at the time that this position is filled or this position change takes place, there may be a difference between the costs projected in this Fiscal impact and the actual costs.
# Request to Refill Position

**Title:** Comprehensive Community Services Case Manager

<table>
<thead>
<tr>
<th>Department</th>
<th>Health and Human Services</th>
<th>Position Title: Comprehensive Community Services Case Manager</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Position Status:</th>
<th>Will be vacant</th>
<th>Date Vacant: May 21, 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Full Time</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reason for Vacancy:</th>
<th>Termination</th>
<th>Transfer</th>
<th>Retirement</th>
<th>Resignation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>☑</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transfer: why is the new position more attractive to employee than current one?

Name of Current / Most Recent Incumbent: Hope Klatt

Reviewed, updated, and submitted to Human Resources:

- ☑ Job Analysis Questionnaire (not to be included in the agenda packet)
- ☑ Job Description

Completed by: Joseph Krebsbach Date: 5-7-21

**Financial Information:**

- Salary Range: $23.33 – $30.53
- Is the Position Budgeted: ☑ Yes ☐ No
- Funding Source: ☐ Levy % ☑ Grant Funded % ☑ Other Medicare and State funding % 100
- ☐ Fiscal Impact, from Finance Department, completed and attached

**HR TO COMPLETE:**

- ☑ EEO Professional
- ☑ FLSA Status: Exempt
- ☑ Human Resources has performed a position review? (HR initial) 5/7/21 Date
- ☑ The Job Description has been updated and signed? (HR initial) 5/7/21 Date

**Approvals:**

- County Administrator: [Signature] Date: 5-7-21
- Administrative Committee Chair: [Signature] Date: 

Date: May 7, 2021
To: Health and Human Services Board
Cc: Administrative Committee; Ken Pabich, County Administrator
RE: Request to Refill Comprehensive Community Services Case Manager

Due to a resignation, we will have a vacancy in our Comprehensive Community Support (CCS) Division as of May 21, 2021. This position provides ongoing coordination of services for individuals or families impacted by mental health and/or substance use issues in CCS as well as Coordinated Services Teams (CST).

We eliminated one position in this program in 2020 when a vacancy occurred, based on caseload at the time. We left that position out of the 2021 budget. During COVID-19 our community has seen an increase in mental health and substance use issues, and consumers are presenting with more complex needs. Our CCS caseload has grown by 10% over the past year, and the CST caseload has grown by 12%. In addition, we currently have another case manager out on Family Medical Leave for 12 weeks. The worker who is leaving is managing a very full caseload, as are all the workers in this division.

The CCS program recoups a combination of state and federal funding that covers our full costs. As a result, there is no local tax levy needed to support this position.

I am requesting permission to refill this position and any subsequent vacancies.
County of Door  
Case Manager – Comprehensive Community Services  
(with On-Call Crisis)

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Case Manager-Comprehensive Community Services</th>
<th>Last Revision</th>
<th>8/9/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Health &amp; Human Services</td>
<td>HR Reviewed</td>
<td></td>
</tr>
<tr>
<td>Division</td>
<td>Behavioral Health/CCS</td>
<td>Employee Group</td>
<td>General Municipal Employee</td>
</tr>
<tr>
<td>Report To</td>
<td>Comprehensive Community Services Program Manager</td>
<td>FLSA Status</td>
<td>Exempt</td>
</tr>
<tr>
<td>Pay Grade</td>
<td></td>
<td>EEO Code</td>
<td>02 – Professionals</td>
</tr>
</tbody>
</table>

General Summary

This advanced position is responsible for a wide range of individualized, client centered, and trauma-informed case management and service facilitation services to individuals across the lifespan affected by mental health and/or substance use problems and to children involved in multiple systems of care. The case manager performs intake functions and screens individuals presenting to the county system for services. The case manager provides assessment, resource development and coordination of services; conducts ongoing monitoring of strengths, needs, and goals; facilitates team meetings; and works with consumers and their teams to develop recovery-focused treatment plans to help individuals receive the most appropriate level of support to achieve their goals.

Duties and Responsibilities

**Essential Job Functions**

1. Develops and maintains knowledge of specific program requirements set forth by Wis. Stats. related to Comprehensive Community Services, Coordinated Services Teams and related programs and services.
2. Conducts necessary screenings and assessments, including AODA/Mental Health functional screen and child functional screens (state screen certified) to determine all program eligibility; completes other state required program documents and tools as assigned.
3. Identifies needs and strengths, and conducts individual assessments regarding the nature of a client’s abilities, disabilities and potential for maximized community and family living.
4. Facilitates team meetings with consumers, providers, family members and other informal supports to develop, implement, and monitor person-centered, recovery-focused treatment plans.
5. Assists clients and families to obtain all available resources (financial, social, remedial) to enable clients to reach established goals and objectives.
6. Monitors, reviews and provides follow-up consultation to ensure client needs are being met.
7. Procures and authorizes services to be delivered by service providers. Monitors the quality and quantity of purchased services to ensure they are consistent with the individual’s goals set forth on the treatment plan and in compliance with authorized hours. Follows up with the provider in a timely manner when adjustments are needed.
8. Prepares and maintains treatment plans and individual progress notes for each assigned client in an electronic record system.
9. Prepares state and federally mandated reports regarding individuals or caseload related to case management functions.
10. Advocates on behalf of clients to ensure needs are met and client rights are protected, enhancing natural supports to the greatest extent possible.
11. Conducts and/or participates in community awareness, education, resource development, and option exploration activities.
12. Provide truthful and accurate written and verbal communications.
County of Door
Case Manager – Comprehensive Community Services
(with On-Call Crisis)

General Job Functions

1. Provides after-hours emergency "On Call" services on rotating basis with other clinical staff.
2. Participates in continuing appropriate professional training.
3. Provides regular supportive contacts with the service providers, team members, and other community partners.
4. Participates in weekly team meetings to review client/clinical supervision issues and receive division program updates.
5. Strictly follows federal and state laws and regulations, county and departmental policies and procedures in regard to privacy, security and confidentiality of individuals' personal and health information.

Requirements

Training and Experience

1. Minimum of Bachelor's degree in Social Work, Psychology, Sociology, Special Education, Human Development or related degree.
2. Two (2) years demonstrated experience working with individuals with behavioral health issues strongly preferred.
3. Current valid Wisconsin driver's license required and access to a reliable standard automobile.

Knowledge, Skills, and Abilities Required

1. Ability to conduct a comprehensive individual assessment, develop individual service plans and activities, and work creatively and independently.
2. Ability to listen carefully, communicate respectfully and engage in conflict resolution and problem-solving.
3. Ability to read, comprehend, and communicate, both orally and in writing, as well as effectively administer program requirements by written and oral communications.
4. Ability to perform basic mathematical calculations; ability to compare invoices to authorizations and service notes and resolve discrepancies.
5. Ability to use tact and courtesy in maintaining an effective working relationship with clients, department employees, county supervisors, county officials, and the general public.
6. Ability to prioritize multiple tasks in an organized, efficient manner.
7. Required to complete 40 hours of state-mandated CCS training within 3 months of hire.
8. Required to complete training and pass Department of Health Services exams to become certified as a functional screener and Child & Adolescent Needs Assessment (CANS) assessor within three months of hire.

Physical & Working Conditions

Nearly 100% of time work is performed in a normal office setting with little or no discomfort from temperature, dust or noise. Interacting with other employees, general public, whether walking in or on the telephone may be encountered.

Over 75% of work is performed seated at a desk, working on a computer keyboard and/or telephone with about 10% of work performed standing and walking. Over 75% of the work is performed by talking, hearing, and using both far and near vision. Occasional lifting is required up to 10 lbs. (i.e. paper and
County of Door
Case Manager – Comprehensive Community Services
(with On-Call Crisis)

Very frequent face to face and over the telephone oral communication with clients, their families and the public. Sitting and standing are required 100% of the time spent on the job. Occasional climbing of stairs.

Work includes driving vehicle to visit clients in their homes and other community settings; interacting with and observing actions of clients to assess needs. Occasional pushing of clients in wheel chairs (20-40 lbs.). Frequent writing or typing of case notes.

In an effort to provide for continuity of County government and to cope with the problems of the emergency, you may be required to work during a proclaimed state of emergency, consistent with Sec 323.14 Wis. Stats. and County emergency management plans and programs.

The above is intended to describe the general content of the requirements for the performance of this job. It is not to be construed as an exhaustive statement of duties, responsibilities or requirements. They may be subject to change at any time due to reasonable accommodation or other reasons.

Approvals:

Joseph A. Krebsbach, Human Services Director

Date

Kelly A. Hendee, Human Services Director

Date
REQUEST FOR FISCAL IMPACT INFORMATION

RECLASSIFICATION

<table>
<thead>
<tr>
<th>FTE/Hours</th>
<th>Job Class</th>
<th>Step</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CHANGE FTE/Hours

<table>
<thead>
<tr>
<th>From</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANGE JOB CLASS/STEP</td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>TO</td>
</tr>
</tbody>
</table>

Position Title  
Effective Date  
Department

<table>
<thead>
<tr>
<th>CCS Case Manager</th>
<th>6 Mo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health &amp; Human Services</td>
<td>Sub Dept</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FTE/Hrs</th>
<th>@ Rate</th>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
<th>TOTAL SALARY and Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS Case Manager-Grade H-Step 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>$23.93</td>
<td>49,908</td>
<td>34,917</td>
<td>84,825</td>
</tr>
<tr>
<td>Budget CCS Case Manager-Grade H-Budget</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>$25.30</td>
<td>52,766</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Salary and Benefit Decrease: (3,383)

<table>
<thead>
<tr>
<th>FTE/Hrs</th>
<th>@ Rate</th>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
<th>TOTAL SALARY and Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS Case Manager-Grade H-Control Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>$27.35</td>
<td>57,041</td>
<td>36,225</td>
<td>93,266</td>
</tr>
<tr>
<td>Budget CCS Case Manager-Grade H-Budget</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>$25.30</td>
<td>52,766</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Salary and Benefit Increase: 5,058

__________________________  ____________________________
Dept Head Signature       Finance Director
5/7/2081

Disclaimer: This Fiscal Impact does not include Step 2 $24.62, Step 3 $25.30, Step 4 $25.98, and Step 5 $26.67.

This Fiscal Impact is an example illustration of what the costs would be for this position/position change. It is based on estimates and assumptions provided by the Human Resources Department and/or the department in which this position works. Because these estimates and assumptions may change, or may be different than the actual circumstances at the time that this position is filled or this position change takes place, there may be a difference between the costs projected in this Fiscal Impact and the actual costs.
Dear Kelly Hendee,

CC: Jamie Cole

Please accept this letter as my formal notification that I am resigning from my position as CCS Service Facilitator. My last day will be 05/21/21. Thank you for the opportunity to work in this position for the last 3 years. I have enjoyed all of my time spent getting to work and support all of the consumers that we have served in my time here, and I’ve learned so much about mental health services and the benefits that they can provide. During my last 2 weeks, I will do everything possible to wrap up my duties and ensure a smooth hand off of consumers that I have been working with.

I have truly enjoyed my time working with the Department and am grateful for all of the experience I have gained throughout my time here.

Sincerely,

Hope Klatt
**Title:** Request to Refill Position

Please reference the most current copy of the Door County Employee Handbook and Administrative Manual.

**DEPT. HEAD TO COMPLETE:**

Department: Library  
Position Title: Library Custodian

Position Status:  
- [x] Currently vacant  
- [ ] Will be vacant  
  
  Date Vacant: 5/22/2021  
  
  [ ] Full Time  
  [x] Part Time  
  [ ] New position  
  Hours per week: 10

Reason for Vacancy:  
- [ ] Termination  
- [ ] Transfer  
- [ ] Retirement  
- [x] Resignation

Transfer: why is the new position more attractive to employee than current one?  
N/A

Name of Current / Most Recent Incumbent: Daniel Miller

Reviewed, updated, and submitted to Human Resources:

- [x] Job Analysis Questionnaire (not to be included in the agenda packet)  
- [x] Job Description

Completed by: Tina Kakuske  
Date 5/2021

**Financial Information:**

Salary Range: 14.28 to 16.32  
Is the Position Budgeted:  
- [x] Yes  
- [ ] No

Funding Source:  
- [ ] Levy  
  %  
- [ ] Grant Funded  
  %  
- [ ] Other  
  %

- [x] Fiscal Impact, from Finance Department, completed and attached

**HR TO COMPLETE:**

- [x] Service/Maintenance  
  FLSA Status: non-exempt

  [KBP] (HR Initial)  
  [5-10-21] Date

- [x] Human Resources has performed a position review?  
  [KBP] (HR Initial)  
  [5-10-21] Date

- [x] The Job Description has been updated and signed?  
  [KBP] (HR Initial)  
  [5-10-21] Date

**Approvals:**

County Administrator  
Date 5-10-21

Library Board President  
Date

Administrative Committee Chair  
Date
General Summary

This position is responsible for general cleaning and custodial duties to maintain library building and grounds in a neat, clean and orderly manner. Sets up furniture in meeting rooms. Closes the library at end of shift. The assistant will also work additional hours in the custodian's absence. Regular attendance and punctuality along with being prepared to commence work at designated work locations, on the assigned or scheduled days and hours is expected.

Duties and Responsibilities

**Essential Job Functions**

1. Snow blowing, snow shoveling, raking and mowing.
2. Cleans restrooms, replacing paper towels, soap and other supplies as necessary.
3. Sets up meeting rooms with tables and chairs arranged for meeting requirements.
5. Empties wastebaskets.
6. Dusts.
7. Replaces light bulbs and cleans fixtures.
8. Washes windows and glass doors.

**General Job Functions**

1. Performs a variety of other custodial tasks as required.

Requirements

**Training and Experience**

1. Experience in custodial work.
2. High school diploma or equivalent.
3. One (1) year of responsible work experience; or an equivalent combination of training and experience desirable.
4. Current valid Wisconsin driver’s license required.
County of Door
Custodian - Library

Knowledge, Skills and Abilities Required

1. Ability to work independently without direct supervision and follow verbal or written instructions.
2. Ability to get along with others.
3. Good knowledge of custodial and maintenance methods and in the use of supplies and equipment.
4. Ability to be thorough and dependable with custodial responsibilities and in good physical condition.
5. Ability to operate basic cleaning equipment: Heavy duty vacuum cleaner, carpet cleaner, snow blower.
6. Ability to lift and move tables, chairs and/or equipment needed to set up meeting rooms.
7. Ability to manipulate rakes and shovels.
8. Ability to bend, twist, reach to clean areas of the library.
9. Ability to climb a tall ladder to replace light bulbs in the main library and to wash high windows.
10. Ability to use tact and courtesy in maintaining an effective working relationship with department employees, county supervisors, county officials, and general public.
11. Ability to read, comprehend, and communicate, both verbally and in writing as well as effectively administer by written, and verbal communications.

Physical & Working Conditions

Most duties in a normal workplace environment or outside in pleasant weather. However, in winter when the library is open the custodian must keep walks and entry clear of snow whatever the temperature or weather.

In an effort to provide for continuity of County government and to cope with the problems of the emergency, you may be required to work during a proclaimed state of emergency, consistent with Sec 323.14 Wis. Stats. and County emergency management plans and programs.

The above is intended to describe the general content of the requirements for the performance of this job. It is not to be construed as an exhaustive statement of duties, responsibilities or requirements. They may be subject to change at any time due to reasonable accommodation or other reasons.

Approvals:

Kristine M. Kakuske, Library Director 5/2/21

Kelly A. Hendee, Human Resources Director 7/3/17

Page 2 of 2
REQUEST FOR FISCAL IMPACT INFORMATION

RECLASSIFICATION

<table>
<thead>
<tr>
<th>FTE/Hours</th>
<th>Job Class</th>
<th>Step</th>
<th>Rate</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Position Title</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Effective Date</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Department</th>
</tr>
</thead>
</table>

Library Custodian

<table>
<thead>
<tr>
<th>2021 TOTAL SALARY</th>
<th>2021 TOTAL BENEFITS</th>
<th>TOTAL SALARY and Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library Custodian-Grade B-Step 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.25</td>
<td>$14.28</td>
<td>7,446</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Budget Library Custodian-Grade B-Budget</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.25</td>
<td>$18.77</td>
<td>9,787</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Library Custodian-Grade B-Step Control Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.25</td>
<td>$16.32</td>
<td>8,509</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Budget Library Custodian-Grade B-Budget</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.25</td>
<td>$18.77</td>
<td>9,787</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Salary and Benefit Decrease</td>
<td>(2,612)</td>
<td></td>
</tr>
<tr>
<td>Total Salary and Benefit Decrease</td>
<td>(1,426)</td>
<td></td>
</tr>
</tbody>
</table>

Dept Head Signature

Finance Director

Date

Disclaimer: This Fiscal Impact does not include Step 2 $14.69, Step 3 $15.10, Step 4 $15.50, and Step 5 $15.91.

This Fiscal Impact is an example illustration of what the costs would be for this position/position change. It is based on estimates and assumptions provided by the Human Resources Department and/or the department in which this position works. Because these estimates and assumptions may change, or may be different than the actual circumstances at the time that this position is filled or this position change takes place, there may be a difference between the costs projected in this Fiscal Impact and the actual costs.
## Separation of Employment

<table>
<thead>
<tr>
<th>Date</th>
<th>Transaction</th>
<th>Department</th>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/06/2021</td>
<td>Resignation</td>
<td>Highway &amp; Airport</td>
<td>Ryan Burntett</td>
<td>Stand by Bridgetender</td>
</tr>
<tr>
<td>04/13/2021</td>
<td>Resignation</td>
<td>Emergency Services</td>
<td>Natasha Phillips</td>
<td>EMT – Stand by</td>
</tr>
<tr>
<td>04/14/2021</td>
<td>Resignation</td>
<td>Emergency Services</td>
<td>Dennis Casey</td>
<td>EMT – Stand by</td>
</tr>
<tr>
<td>04/29/2021</td>
<td>Resignation</td>
<td>H&amp;HS (Public Health)</td>
<td>Kendra Vanderlie</td>
<td>LTE Contact Tracer</td>
</tr>
<tr>
<td>05/01/2021</td>
<td>Resignation</td>
<td>Library</td>
<td>Danial Miller</td>
<td>Custodian – Library</td>
</tr>
<tr>
<td>05/03/2021</td>
<td>Resignation</td>
<td>EM&amp;C</td>
<td>Linda Nault</td>
<td>LTE Telecommunicator</td>
</tr>
<tr>
<td>05/04/2021</td>
<td>Resignation</td>
<td>Child Support</td>
<td>Sara Krouse</td>
<td>Child Support Specialist</td>
</tr>
<tr>
<td>05/21/2021</td>
<td>Resignation</td>
<td>Health &amp; Human Services</td>
<td>Hope Klatt</td>
<td>CC3 Case Manager</td>
</tr>
<tr>
<td>07/01/2021</td>
<td>Retirement</td>
<td>Sheriff's Office</td>
<td>Timothy Fuerst</td>
<td>Patrol Deputy</td>
</tr>
</tbody>
</table>

## New Hires

<table>
<thead>
<tr>
<th>Date</th>
<th>Transaction</th>
<th>Department</th>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/08/2021</td>
<td>Internal Hire</td>
<td>Museum</td>
<td>Steven Rice</td>
<td>Museum &amp; Archives Manager</td>
</tr>
<tr>
<td>04/09/2021</td>
<td>Hired</td>
<td>H&amp;HS (Public Health)</td>
<td>Cynthia Regnier</td>
<td>Public Health Nurse (LTE)</td>
</tr>
<tr>
<td>04/19/2021</td>
<td>Re-hired</td>
<td>Facilities &amp; Parks</td>
<td>Mark Larson</td>
<td>Seasonal – Parks</td>
</tr>
<tr>
<td>04/20/2021</td>
<td>Hired</td>
<td>Emergency Services</td>
<td>Lauren Junion</td>
<td>EMT Stand by</td>
</tr>
<tr>
<td>04/20/2021</td>
<td>Hired</td>
<td>Emergency Services</td>
<td>Samantha LaLuzerne</td>
<td>EMT Stand by</td>
</tr>
<tr>
<td>04/29/2021</td>
<td>Internal Hire</td>
<td>Circuit Court</td>
<td>Pamela Parks</td>
<td>Judicial Assistant</td>
</tr>
<tr>
<td>04/28/2021</td>
<td>Hired</td>
<td>H&amp;HS (ADRC)</td>
<td>Ronald Niesing</td>
<td>LTE – Disability Benefit Specialist</td>
</tr>
<tr>
<td>05/03/2021</td>
<td>Re-hired</td>
<td>Facilities &amp; Parks</td>
<td>John Puetz</td>
<td>Seasonal - Parks</td>
</tr>
<tr>
<td>05/10/2021</td>
<td>Re-hired</td>
<td>Facilities &amp; Parks</td>
<td>Heather Truett</td>
<td>Seasonal – Parks</td>
</tr>
<tr>
<td>05/10/2021</td>
<td>Hired</td>
<td>Highway &amp; Airport</td>
<td>Joshua Nolan</td>
<td>Seasonal - Highway</td>
</tr>
<tr>
<td>05/10/2021</td>
<td>Re-hired</td>
<td>Highway &amp; Airport</td>
<td>Craig Weis</td>
<td>Seasonal - Airport</td>
</tr>
<tr>
<td>05/10/2021</td>
<td>Hired</td>
<td>Highway &amp; Airport</td>
<td>Jamie Jelinek</td>
<td>Highway Worker</td>
</tr>
<tr>
<td>05/12/2021</td>
<td>Hired</td>
<td>Transportation</td>
<td>Gary Hanson</td>
<td>LTE Bus Driver</td>
</tr>
<tr>
<td>05/12/2021</td>
<td>Re-hired</td>
<td>Facilities &amp; Parks</td>
<td>Kristin Rankin</td>
<td>Seasonal – Parks</td>
</tr>
<tr>
<td>05/14/2021</td>
<td>Hired</td>
<td>H&amp;HS (Public Health)</td>
<td>Amy Jacobs</td>
<td>Public Health Nurse (LTE)</td>
</tr>
<tr>
<td>05/17/2021</td>
<td>Hired</td>
<td>Highway &amp; Airport</td>
<td>Alexis Jandrin</td>
<td>Seasonal – Highway</td>
</tr>
<tr>
<td>05/17/2021</td>
<td>Hired</td>
<td>Highway &amp; Airport</td>
<td>Alexis Jandrin</td>
<td>Seasonal – Highway</td>
</tr>
<tr>
<td>05/19/2021</td>
<td>Hired</td>
<td>Highway &amp; Airport</td>
<td>Jeremy Schopf</td>
<td>Mechanic</td>
</tr>
<tr>
<td>05/24/2021</td>
<td>Hired</td>
<td>Facilities &amp; Parks</td>
<td>Bruce Anschutz</td>
<td>Seasonal – Parks</td>
</tr>
<tr>
<td>06/01/2021</td>
<td>Hired</td>
<td>Highway &amp; Airport</td>
<td>David Lloyd</td>
<td>Seasonal – Highway</td>
</tr>
</tbody>
</table>

## Introductory Period Completion

<table>
<thead>
<tr>
<th>Date</th>
<th>Transaction</th>
<th>Department</th>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/17/2021</td>
<td></td>
<td>Library</td>
<td>Sandra McGrath</td>
<td>Circulation Assistant</td>
</tr>
</tbody>
</table>

## Table Definitions
- **Hired**: Newly hired employees
- **Inactive**: Regular, Limited Term and Seasonal Employees no longer working (separated from employment)
- **Internal Hire**: Candidate selected from another department within the organization.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-Hired</td>
<td>Former Employees returning to employment in same category as originally hired. (Seasonal)</td>
</tr>
<tr>
<td>Resignation</td>
<td>Employees submitted correspondence indicating they are leaving employment and not retirement eligible.</td>
</tr>
<tr>
<td>Retirement</td>
<td>Employees qualified to retire because of &quot;eligible years of service&quot; or &quot;eligible retirement age&quot;.</td>
</tr>
<tr>
<td>Termination</td>
<td>Employer terminates employment with employee (includes layoff)</td>
</tr>
<tr>
<td>Intro</td>
<td>Completion of introduction period</td>
</tr>
</tbody>
</table>
## Accounts Payable Invoice Report

**Payment Date Range**: 04/01/21 - 04/30/21

**Report By Department**: 14 - Corporation Counsel

### Summary Listing

<table>
<thead>
<tr>
<th>Invoice Number</th>
<th>Invoice Description</th>
<th>Status</th>
<th>Held Reason</th>
<th>Invoice Date</th>
<th>Due Date</th>
<th>G/L Date</th>
<th>Received Date</th>
<th>Payment Date</th>
<th>Invoice Net Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sub-Department 14 Corporation Counsel Totals</td>
<td>Invoices</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor 36721 - WEST GROUP PAYMENT CENTER Totals</td>
<td>Invoices</td>
<td>1</td>
<td></td>
<td>1,677.56</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Batch Number 2021-00000237 Totals</td>
<td>Invoices</td>
<td>1</td>
<td></td>
<td>1,677.56</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department 14 - Corporation Counsel Totals</td>
<td>Invoices</td>
<td>3</td>
<td></td>
<td>3,312.72</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-2021</td>
<td>March 2021 Mediation Services</td>
<td>Paid by Check #681768</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/08/2021</td>
<td>1,525.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sub-Department 14 Corporation Counsel Totals</td>
<td>Invoices</td>
<td>1</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor 8852 - GAY PUSTAVER Totals</td>
<td>Invoices</td>
<td>1</td>
<td></td>
<td>$1,525.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>130414</td>
<td>March 2021 Copier Costs</td>
<td>Paid by Check #681769</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/08/2021</td>
<td>110.16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sub-Department 14 Corporation Counsel Totals</td>
<td>Invoices</td>
<td>1</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor 5999 - WISCONSIN DOCUMENT IMAGING Totals</td>
<td>Invoices</td>
<td>1</td>
<td></td>
<td>$110.16</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Vendor Details

**Vendor**: 8852 - GAY PUSTAVER
- **Department**: 14 Corporation Counsel
- **Batch Number**: 2021-00000208
- **Status**: Batch Date 04/09/2021
- **Entered by**: User Amanda Sawdo

**Vendor**: 5999 - WISCONSIN DOCUMENT IMAGING
- **Department**: 14 Corporation Counsel
- **Sub-Department**: 14 Corporation Counsel
- **Batch Number**: 2021-00000237
- **Status**: Batch Date 04/23/2021
- **Entered by**: User Amanda Sawdo

---

Run by Amanda Sawdo on 05/10/2021 09:37:41 AM
<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
<th>Prepaid</th>
</tr>
</thead>
<tbody>
<tr>
<td>53106</td>
<td>AMAZON CAPITAL SERVICE</td>
<td>OFFICE SUPPLIES</td>
<td>$17.84</td>
<td></td>
</tr>
<tr>
<td>52412</td>
<td>DNA DIAGNOSTICS CENTER</td>
<td>PATERNITY BLOOD TESTS</td>
<td>$72.00</td>
<td></td>
</tr>
<tr>
<td>53106</td>
<td>SAFEGUARD</td>
<td>OFFICE SUPPLIES</td>
<td>$69.27</td>
<td></td>
</tr>
<tr>
<td>52302</td>
<td>VILLA REAL</td>
<td>SERVICE CONTRACT</td>
<td>$81.25</td>
<td></td>
</tr>
<tr>
<td>52302</td>
<td>WISCONSIN DOCUMENT</td>
<td>SERVICE CONTRACT</td>
<td>$206.88</td>
<td></td>
</tr>
</tbody>
</table>

**PRE-PAID**

<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
<th>Prepaid</th>
</tr>
</thead>
<tbody>
<tr>
<td>52302</td>
<td>DOOR COUNTY SHERIFF</td>
<td>SERVICE CONTRACT</td>
<td>$130.00</td>
<td>JE</td>
</tr>
</tbody>
</table>

**TOTAL:** $577.24

I hereby approve payment of the monthly bills for the CHILD SUPPORT ENFORCEMENT AGENCY as listed on this document.

Date: ______________________

_________________________________
Chairman
Administrative Services Committee
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Invoice No.</th>
<th>Invoice Description</th>
<th>Status</th>
<th>Held Reason</th>
<th>Invoice Date</th>
<th>Due Date</th>
<th>G/L Date</th>
<th>Received Date</th>
<th>Payment Date</th>
<th>Invoice Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>8482</td>
<td>2021-0000157</td>
<td>ATTORNEY RICK MEIER Court Appointed Attorney Fees</td>
<td>Paid by Check # 682300</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$843.55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3629</td>
<td>2021-0000117</td>
<td>PRIBYL LAW S.C. Court Appointed Attorney Fees</td>
<td>Paid by Check # 681878</td>
<td>04/01/2021</td>
<td>04/02/2021</td>
<td>04/02/2021</td>
<td>04/09/2021</td>
<td>$3,390.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14343</td>
<td>2021-0000154</td>
<td>BLAZKOVEC, BLAZKOVEC &amp; DOWNEY Court Appointed Attorney Fees</td>
<td>Paid by Check # 682301</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$420.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1340</td>
<td>2021-0000156</td>
<td>NINA MARTEL SC Court Appointed Attorney Fees</td>
<td>Paid by Check # 682303</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$829.53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9682</td>
<td>2021-0000158</td>
<td>PINKERT LAW FIRM LLP Court Appointed Attorney Fees</td>
<td>Paid by Check # 682304</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$20.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1967</td>
<td>2021-0000115</td>
<td>CAMERA CORNER Crestron Repairs - Branch 1</td>
<td>Paid by Check # 681876</td>
<td>04/01/2021</td>
<td>04/02/2021</td>
<td>04/02/2021</td>
<td>04/09/2021</td>
<td>$472.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21104</td>
<td>2021-0000116</td>
<td>JV TRANSLATOR, LLC Interpreter Fees</td>
<td>Paid by Check # 681877</td>
<td>04/01/2021</td>
<td>04/02/2021</td>
<td>04/02/2021</td>
<td>04/09/2021</td>
<td>$100.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15825</td>
<td>2021-0000118</td>
<td>SUSAN G RASCON Interpreter Fees</td>
<td>Paid by Check # 681880</td>
<td>04/01/2021</td>
<td>04/02/2021</td>
<td>04/02/2021</td>
<td>04/09/2021</td>
<td>$200.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13733</td>
<td>2021-0000120</td>
<td>SWITS, LTD Interpreter Fees</td>
<td>Paid by Check # 681881</td>
<td>04/01/2021</td>
<td>04/02/2021</td>
<td>04/02/2021</td>
<td>04/09/2021</td>
<td>$75.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21104</td>
<td>2021-0000155</td>
<td>JV TRANSLATOR, LLC Interpreter Fees</td>
<td>Paid by Check # 682302</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$222.42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15825</td>
<td>2021-0000159</td>
<td>SUSAN G RASCON Interpreter Fees</td>
<td>Paid by Check # 682306</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$100.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13733</td>
<td>2021-0000161</td>
<td>SWITS, LTD Interpreter Fees</td>
<td>Paid by Check # 682307</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$98.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15069</td>
<td>2021-0000119</td>
<td>STAPLES ADVANTAGE Office Supplies</td>
<td>Paid by Check # 681879</td>
<td>04/01/2021</td>
<td>04/02/2021</td>
<td>04/02/2021</td>
<td>04/09/2021</td>
<td>$224.44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15069</td>
<td>2021-0000160</td>
<td>STAPLES ADVANTAGE Office Supplies</td>
<td>Paid by Check # 682305</td>
<td>04/22/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/27/2021</td>
<td>$142.35</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Grand Totals: $7,138.29
### COUNTY BOARD or OTHER VOUCHERS:

<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
<th>Prepaid</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.39.1351.52401</td>
<td>Brown County Treasurer</td>
<td>Interagency Fee - None this month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.11.1101.53101</td>
<td>Staples Business Advantage</td>
<td>Office Supplies</td>
<td>$116.74</td>
<td>X</td>
</tr>
<tr>
<td>various</td>
<td>Cardmember Service</td>
<td>D/K Legislative Day food, County Board Lunch, Office Supplies</td>
<td>$1,074.50</td>
<td>X</td>
</tr>
<tr>
<td>100.49.1115.52402</td>
<td>Rotary Club of Sturgeon Bay</td>
<td>Quarterly membership Apr-June K. Pabich</td>
<td>$200.00</td>
<td>X</td>
</tr>
<tr>
<td>100.39.1351.52401</td>
<td>Washington Island Ferry Line</td>
<td>Special Ferry (Medical Examiner) (none)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### County Administrator Vouchers:

<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
<th>Prepaid</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.49.1115.53106</td>
<td>Staples Business Advantage</td>
<td>none this month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.49.115.54102</td>
<td>Cardmember Service</td>
<td>none this month</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Transportation Vouchers:

<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
<th>Prepaid</th>
</tr>
</thead>
<tbody>
<tr>
<td>71-Transportation</td>
<td>Cellcom Wisconsin RSA 10</td>
<td>April 2021 Cell charges</td>
<td>$46.07</td>
<td>X</td>
</tr>
<tr>
<td>71-Transportation</td>
<td>Boettcher Communications</td>
<td>Feb/Mar 2021 Marketing</td>
<td>$80.00</td>
<td>X</td>
</tr>
<tr>
<td>71-Transportation</td>
<td>Amazon Capital Services</td>
<td>Flex Rte Supplies</td>
<td>$332.00</td>
<td>X</td>
</tr>
<tr>
<td>71-Transportation</td>
<td>J.B. Truck Service LLC</td>
<td>Bus repairs due to shake in front</td>
<td>$1,188.40</td>
<td>X</td>
</tr>
<tr>
<td>71-Transportation</td>
<td>Abby Vans</td>
<td>March 2021 D2D Taxi</td>
<td>$49,847.48</td>
<td>X</td>
</tr>
<tr>
<td>71-Transportation</td>
<td>Jim Olson Chrysler</td>
<td>O/C and Tire Rotate-Van</td>
<td>$54.95</td>
<td>X</td>
</tr>
<tr>
<td>71-Transportation</td>
<td>Staples Advantage</td>
<td>Flex Rte items</td>
<td>$22.69</td>
<td>X</td>
</tr>
</tbody>
</table>

**TOTAL:** $52,962.83
<table>
<thead>
<tr>
<th>Invoice Number</th>
<th>Invoice Description</th>
<th>Status</th>
<th>Held Reason</th>
<th>Invoice Date</th>
<th>Due Date</th>
<th>G/L Date</th>
<th>Received Date</th>
<th>Payment Date</th>
<th>Invoice Net Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>3473030603</td>
<td>Cty Clerk - Office Supplies</td>
<td>Paid by Check #682196</td>
<td>04/22/2021</td>
<td>04/22/2021</td>
<td>04/22/2021</td>
<td>04/26/2021</td>
<td></td>
<td></td>
<td>48.76</td>
</tr>
</tbody>
</table>

**Department:** 10 - County Clerk
**Vendor:** 15069 - STAPLES ADVANTAGE
**Sub-Department:** 10 County Clerk
**Batch Number:** 2021-00000253
**Batch Date:** 04/22/2021
**Entered by User:** Barb Pavlik

---

**10 County Clerk**

---

**Grand Totals:**
- **Invoices:** 1
- **Grand Total:** $48.76
<table>
<thead>
<tr>
<th>Invoice Number</th>
<th>Invoice Description</th>
<th>Vendor</th>
<th>Sub-Department</th>
<th>Status</th>
<th>Invoice Date</th>
<th>Due Date</th>
<th>G/L Date</th>
<th>Received Date</th>
<th>Payment Date</th>
<th>Invoice Net Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>9344</td>
<td>20GN31 Guardian ad Litem</td>
<td>14343 - B LAZKOVEC, B LAZKOVEC &amp; DOWNEY</td>
<td>25 Court Systems</td>
<td>Edit</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>250.00</td>
</tr>
<tr>
<td>1875.00</td>
<td>Evaluations, travel and testimony</td>
<td>2288 - KEYSTONE PSYCHOLOGY LLC</td>
<td>25 Court Systems</td>
<td>Edit</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>1,875.00</td>
</tr>
<tr>
<td>19814121</td>
<td>Transcripts</td>
<td>2674 - LISA A HARTEL</td>
<td>25 Court Systems</td>
<td>Edit</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>46.50</td>
</tr>
<tr>
<td>213</td>
<td>Guardian ad Litem fees</td>
<td>20086 - MARSHALL J BALES</td>
<td>25 Court Systems</td>
<td>Edit</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>1,156.66</td>
</tr>
<tr>
<td>19114142021</td>
<td>Guardian ad Litem fees</td>
<td>15303 - NINA MARTEL SC</td>
<td>25 Court Systems</td>
<td>Edit</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>939.42</td>
</tr>
<tr>
<td>530201127</td>
<td>Guardian ad Litem fees</td>
<td>9682 - PINKERT LAW FIRM LLP</td>
<td>25 Court Systems</td>
<td>Edit</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>250.00</td>
</tr>
<tr>
<td>Invoice Number</td>
<td>Invoice Description</td>
<td>Status</td>
<td>Vendor</td>
<td>Sub-Department</td>
<td>Invoice Date</td>
<td>Due Date</td>
<td>G/L Date</td>
<td>Received Date</td>
<td>Payment Date</td>
<td>Invoice Net Amount</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
<td>--------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>11841</td>
<td>Guardian ad Litem fees</td>
<td>Edit</td>
<td>Vendor 3629 - PRIBYL LAW S.C.</td>
<td>25 Court Systems</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>370.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor 3629 - PRIBYL LAW S.C. Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$370.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-45</td>
<td>21ME11 Evaluation</td>
<td>Edit</td>
<td>Vendor 11151 - SANGITA PATEL MD</td>
<td>25 Court Systems</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>750.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor 11151 - SANGITA PATEL MD Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$750.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3473158961</td>
<td>toner cartridge for printer</td>
<td>Edit</td>
<td>Vendor 15069 - STAPLES ADVANTAGE</td>
<td>25 Court Systems</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>148.79</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor 15069 - STAPLES ADVANTAGE Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$148.79</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5090789</td>
<td>2021 Lawyer Directory</td>
<td>Edit</td>
<td>Vendor 17463 - STATE BAR OF WISCONSIN</td>
<td>25 Court Systems</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>24.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor 17463 - STATE BAR OF WISCONSIN Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$24.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>844184362</td>
<td>library plan charges</td>
<td>Edit</td>
<td>Vendor 36721 - WEST GROUP PAYMENT CENTER</td>
<td>25 Court Systems</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>1,205.34</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor 36721 - WEST GROUP PAYMENT CENTER Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$1,205.34</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>130426</td>
<td>March 2021 copier lease</td>
<td>Edit</td>
<td>Vendor 5999 - WISCONSIN DOCUMENT IMAGING</td>
<td>25 Court Systems</td>
<td>04/21/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td></td>
<td></td>
<td>197.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor 5999 - WISCONSIN DOCUMENT IMAGING Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$197.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-Department 25 Court Systems Totals</td>
<td></td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Batch Number 2021-00000252</td>
<td></td>
<td>Invoices 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$7,768.51</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Department 25 - Court Systems</td>
<td></td>
<td>Invoices 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

25 Court Systems ___________________________________________________  

Grand Totals Invoices 13  

$7,768.51
<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>52408</td>
<td>Patrick L. Zelzer</td>
<td>Process Service</td>
<td>$75.00</td>
</tr>
<tr>
<td>53106</td>
<td>Staples Advantage</td>
<td>Office Supplies</td>
<td>$470.30</td>
</tr>
<tr>
<td>53183</td>
<td>Staples Advantage</td>
<td>Data Processing Supplies</td>
<td>$91.44</td>
</tr>
<tr>
<td>53109</td>
<td>West Group</td>
<td>Publications</td>
<td>$41.26</td>
</tr>
</tbody>
</table>

TOTAL: $678.00

I hereby approve payment of the monthly bills for the DISTRICT ATTORNEY’S OFFICE as listed on this document.

Dated: ____________________

_______________________________________
Chairman
Administrative Services Committee
<table>
<thead>
<tr>
<th>Invoice Number</th>
<th>Invoice Description</th>
<th>Status</th>
<th>Held Reason</th>
<th>Invoice Date</th>
<th>Due Date</th>
<th>G/L Date</th>
<th>Received Date</th>
<th>Payment Date</th>
<th>Invoice Net Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>350088</td>
<td>Professional Services thru February 2021</td>
<td>Paid by Check #681770</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/08/2021</td>
<td>450.00</td>
<td></td>
</tr>
<tr>
<td>5999 - WISCONSIN DOCUMENT IMAGING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5999 - WISCONSIN DOCUMENT IMAGING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$450.00</td>
</tr>
<tr>
<td>130352</td>
<td>Copier Staples Refill</td>
<td>Paid by Check #681771</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/08/2021</td>
<td>44.81</td>
<td></td>
</tr>
<tr>
<td>130418</td>
<td>March 2021 Copier Costs</td>
<td>Paid by Check #681771</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/08/2021</td>
<td>357.53</td>
<td></td>
</tr>
<tr>
<td>18106 - AURORA HEALTH CARE, INC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18106 - AURORA HEALTH CARE, INC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$852.34</td>
</tr>
<tr>
<td>23287</td>
<td>Quarterly 4/1/2021-6/30/2021</td>
<td>Paid by Check #681886</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/12/2021</td>
<td>1,394.64</td>
<td></td>
</tr>
<tr>
<td>23281</td>
<td>Classified</td>
<td>Paid by Check #681887</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/12/2021</td>
<td>854.82</td>
<td></td>
</tr>
<tr>
<td>12533 - PREVEA HEALTH OCCUPATIONAL HEALTH</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12533 - PREVEA HEALTH OCCUPATIONAL HEALTH</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$854.82</td>
</tr>
<tr>
<td>3005</td>
<td>Pre-Work Screening</td>
<td>Paid by Check #681888</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/12/2021</td>
<td>588.35</td>
<td></td>
</tr>
<tr>
<td>4331 - WI DEPT OF JUSTICE CRIME INFO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4331 - WI DEPT OF JUSTICE CRIME INFO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$588.35</td>
</tr>
<tr>
<td>202103</td>
<td>Background Checks</td>
<td>Paid by Check #681889</td>
<td></td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/09/2021</td>
<td>04/12/2021</td>
<td>30.00</td>
<td></td>
</tr>
<tr>
<td>Invoice Number</td>
<td>Invoice Description</td>
<td>Status</td>
<td>Held Reason</td>
<td>Invoice Date</td>
<td>Due Date</td>
<td>G/L Date</td>
<td>Received Date</td>
<td>Payment Date</td>
<td>Invoice Net Amount</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------------</td>
<td>-----------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>2021-00000230</td>
<td>44 Human Resources</td>
<td>Batch Date</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/15/2021</td>
<td></td>
<td></td>
<td>134.00</td>
</tr>
<tr>
<td>2717 - BELLIN HEALTH</td>
<td>Pre-Work Screening</td>
<td>Paid by Check #682090</td>
<td>Sub-Department 44 Human Resources Totals</td>
<td>Invoices 1</td>
<td>0</td>
<td></td>
<td></td>
<td>$134.00</td>
<td></td>
</tr>
<tr>
<td>2021-00000242</td>
<td>44 Human Resources</td>
<td>Batch Date</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/23/2021</td>
<td>04/15/2021</td>
<td></td>
<td></td>
<td>9,897.51</td>
</tr>
<tr>
<td>523 - MINNESOTA LIFE INSURANCE COMPA</td>
<td>May 2021 Life Insurance Payment</td>
<td>Paid by Check #682091</td>
<td>Sub-Department 44 Human Resources Totals</td>
<td>Invoices 1</td>
<td>0</td>
<td></td>
<td></td>
<td>$9,897.51</td>
<td></td>
</tr>
<tr>
<td>2021-00000230</td>
<td>44 Human Resources</td>
<td>Batch Number 2021-00000230 Totals</td>
<td>Invoices 2</td>
<td></td>
<td></td>
<td>10,031.51</td>
<td></td>
<td></td>
<td>$10,031.51</td>
</tr>
<tr>
<td>6979 - CARLSON DETTMANN CONSULTING</td>
<td>Travel Expenses - Consultant</td>
<td>Paid by Check #682192</td>
<td>Sub-Department 44 Human Resources Totals</td>
<td>Invoices 1</td>
<td>0</td>
<td></td>
<td></td>
<td>182.31</td>
<td></td>
</tr>
<tr>
<td>44 Human Resources</td>
<td>6979 - CARLSON DETTMANN CONSULTING</td>
<td>Vendor Totals</td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td>$182.31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18272 - DOOR COUNTY MEDICAL CENTER</td>
<td>Chair Massages</td>
<td>Paid by Check #682193</td>
<td>Sub-Department 44 Human Resources Totals</td>
<td>Invoices 1</td>
<td>0</td>
<td></td>
<td></td>
<td>160.00</td>
<td></td>
</tr>
<tr>
<td>44 Human Resources</td>
<td>18272 - DOOR COUNTY MEDICAL CENTER</td>
<td>Vendor Totals</td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td>$160.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10321 - HRI, DBA: HUMANNA WELLNESS</td>
<td>Administrative Services</td>
<td>Paid by Check #682194</td>
<td>Sub-Department 44 Human Resources Totals</td>
<td>Invoices 1</td>
<td>0</td>
<td></td>
<td></td>
<td>5,386.00</td>
<td></td>
</tr>
<tr>
<td>44 Human Resources</td>
<td>10321 - HRI, DBA: HUMANNA WELLNESS</td>
<td>Vendor Totals</td>
<td>Invoices 1</td>
<td></td>
<td></td>
<td>$5,386.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021-00000242</td>
<td>44 Human Resources</td>
<td>Batch Number 2021-00000242 Totals</td>
<td>Invoices 3</td>
<td></td>
<td></td>
<td>$5,728.31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44 Human Resources</td>
<td>Grand Totals</td>
<td>Invoices 12</td>
<td></td>
<td></td>
<td></td>
<td>$19,479.97</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Run by Amanda Sawdo on 05/10/2021 09:32:29 AM
<table>
<thead>
<tr>
<th>Acct No.</th>
<th>Vendor</th>
<th>Description</th>
<th>Amount</th>
<th>Prepaid</th>
</tr>
</thead>
<tbody>
<tr>
<td>52206</td>
<td>Cellcom</td>
<td>Monthly Cellcom Charges</td>
<td>$76.61</td>
<td>x</td>
</tr>
<tr>
<td>58129</td>
<td>Door-Tran</td>
<td>Veteran Transport from Bellin</td>
<td>$60.00</td>
<td>x</td>
</tr>
<tr>
<td>58129</td>
<td>Door-Tran</td>
<td>Vet Transport to/from GB VA Clinic</td>
<td>$200.00</td>
<td>x</td>
</tr>
<tr>
<td>59117</td>
<td>DC Emergency Services</td>
<td>Ambulance Bill for Vet</td>
<td>$1,334.00</td>
<td>x</td>
</tr>
</tbody>
</table>

**TOTAL:** $1,670.61

I hereby approve payment of the monthly bills for the VETERANS SERVICE OFFICE as listed on this document.

Date: ________________________

________________________________________
David Lienau, Chairman
Administrative Committee