

Emergency Services of Door County recognizes its obligation under the **Health Insurance Portability and Accountability Act (HIPAA)**. The following are the HIPAA policies and procedures specific to the Emergency Services Department.

Compliance

Emergency Services of Door County intends to fully comply with all aspects and requirements of HIPAA. Further, the department obligates all employees and business associates to the same commitment of compliance. Failure by employees to comply with this policy may result in disciplinary action as indicated by Door County's disciplinary procedure or by the disciplinary procedure identified in the appropriate Union contract. Failure by a business associate to comply with HIPAA policies will result in a termination of the association with that business.

Training

A. New Hires

During the orientation phase of employment, all new employees will receive training in HIPAA. Following the training, the newly hired employees will be expected to sign the staff member verification document.

B. Existing Personnel

All Emergency Services employees will receive training on HIPAA annually. Following the training session, employees will be expected to sign the staff member verification document attached and identified as Appendix A.

Confidentiality

A. Verbal

All conversations with patients or others specific to a patient's condition are considered confidential. Employees of Emergency Services of Door County are not to share the content of those conversations with anyone except as permitted, or as ordered by law.

B. Written

All written documentation of patient condition is considered confidential. Employees of Emergency Services of Door County are not to share the content of the written documentation with anyone except as permitted, or ordered by law.

Written reports

Written reports are to be sealed and/or secured after the completion of the report and are to be accessed by only those on a need to know basis. The following people (positions) have rights to access written protected healthcare information:

1. Medics involved with the run
2. Emergency Services Clerk Typist for data entry, billing and accounts receivable information
3. Patient Account Specialist for data entry, billing and accounts receivable information
4. Administrative Assistant for data entry, billing and accounts receivable information
5. Director of Services for quality assurance, data entry, billing and accounts receivable
6. Medical Director for quality assurance

Written reports are not to be placed or left in an area that is accessible by other individuals than those listed as having any right to access. All reports are to be secured at the end of the workday.

Computer Reports

All computer documentation pertaining to a patient is considered confidential. Employees of Emergency Services of Door County are not to share the content of the computer report with anyone except as permitted, or ordered by law. The following people/positions have a right to access protected health care computer information.

1. Medics involved with the run
2. Emergency Services Clerk Typist for data entry, billing and accounts receivable information
3. Patient Account Specialist for data entry, billing and accounts receivable information
4. Administrative Assistant for data entry, billing and accounts receivable information
5. Director of Services for quality assurance, data entry, billing and accounts receivable
6. Medical Director for quality assurance

Computers that contain protected health care information are to have a screen saver component that initializes after two minutes of inactivity. Following initialization, access back into the system is to be with a password.

Password Protection

Password Protection of computers is per Door County Password Protection Policy attached and identified as Appendix B.

Notice of Privacy

- A. All patients treated and/or transported by Emergency Services of Door County are to be given a copy of Door County's "Notice of Privacy Protections" attached and identified as Appendix C.
- B. To acknowledge receipt of this document, medics are to secure the signature of the patient or the patient's family. If the patient is unable to sign and there is no family to sign, the medic should sign indicating that the materials were left with the patient. The signature card is attached and identified as Appendix D.

Privacy Officer

As required by law, Door County is obligated to identify a Privacy Officer specific to the requirements of HIPAA. Door County's Privacy Officer is the County's Corporation Counsel. The Privacy Officer in Door County identifies a contact person in each department with HIPAA obligations. In the Emergency Services department, the Director is identified as the contact person. The responsibility of the contact person includes the following:

1. The contact person is required to assure that training is done on an annual basis with all those required to be trained.
2. The contact person is the person to release information when a release of information is requested and when the release is determined to be appropriate.
3. The contact person is the person who assures the department is meeting the obligations of the department.

If an employee or lay person has a complaint or concern regarding a HIPAA issue and is not satisfied with the response of the contact person at Emergency Services, he/she should take the concern to the Door County Corporation Counsel.

Suzi Derenne	Date	Verona Robillard	Date
Chris Jeanquart	Date	Andy Rutz	Date
Ken Long	Date	Tony Rutz	Date
Jim Olson	Date	Angie Spude	Date
Ann Schartner	Date	Dennis Tremble	Date
Mark Dewey	Date	Becky Tremble	Date
Debbie Dahms	Date	Curt Vandertie	Date
Mary Dart	Date	Bev Wautier	Date
Rena LaLuzerne	Date	Jeffrey Routhieaux	Date
Robyn Paye	Date	Dawn Routhieaux	Date
Chris Hecht	Date	Anne Alberts	Date
Greg Diltz	Date	Ken Bittorf	Date
Aaron LeClair	Date	Julie Williams	Date
Michelle Bubnick	Date	Bob Landeck	Date
Brandon Schopf	Date		Date
	Date		Date
	Date		Date
	Date		Date
	Date		Date
	Date		Date
	Date		Date
	Date		Date
	Date		Date

Appendix A
TRAINING DOCUMENTATION

HIPAA Privacy Rules require that a covered entity's employees with access to Protected Health Information (PHI) must be trained on the entity's policies and procedures regarding PHI. The objective of training is to ensure those individuals receiving, using or disclosing PHI understand their responsibilities under the rules and regulations of HIPAA. By signing this document, the undersigned acknowledges an understanding of his/her duties as required by HIPAA and receipt of training regarding Door County's privacy policies and procedures. The undersigned also acknowledges receipt of Door County's Notice of Privacy Practices.

Name of Employee (Printed)

Signature of Employee

Date of Training Received

Type of Training
Received: _____

Appendix B

318.5 - PASSWORD POLICY

I. PURPOSE:

This policy outlines the use, responsibilities, and scope of passwords used to gain access to Information System resources belonging to the County of Door. Passwords are the entry point to Door County's information system resources. Protecting access to these resources is crucial to ensuring that 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.

II. Systems Involved and Frequency of Change:

- A. **Network connection:** Windows username and password will automatically be prompted at a login to change the password every eight weeks.
- B. **AIX/Unix password:** Users of the Door County Public Safety system will automatically be prompted to change their password every eight weeks.
- C. **AS400 profile password:** All IBM AS400 users will be prompted to change their profile password every eight weeks.
- D. **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.
- E. **Third party applications:** Contact the Information Systems Department (IS) employee acting as the administrator for the application to determine specific password requirements. Some examples include the New World Systems (NWS) Financial package and The Clinical Manager application in Community Programs.
- F. **State applications:** Contact your State representative for specific password requirements.
- G. **Internet applications:** These applications may or may not have password requirements. Contact the application or service provider for specific password requirements. Some examples include WILENET and eTIME.
- H. **Computer BIOS password:** The password for hardware-level access to your computer will not automatically change and shall be controlled by IS personnel ONLY.

III. Password Usage:

Passwords for **all** systems are subject to the following rules:

- A. 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.
- B. No passwords are to be shared in order to replace an employee who is out of the office. The employee's supervisor shall contact Information Systems, and request a temporary account or appropriate changes to permissions if there are resources that the person needs to access.
- C. Passwords are not to be displayed or concealed anywhere in the employee's workspace.
- D. Users must use a minimum of ten unique passwords before the first password can be repeated.

IV. Password Composition:

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.

- A. User passwords must meet the following minimum criteria:
 - 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.
 - 2. Password must be at least six characters long.
 - 3. Password shall contain no repeated characters side by side.

- B. Additional recommendations:
 - 1. Use both upper and lower case letters.
 - 2. Note: Most systems accept upper and lower case and those that do not will just ignore the letter's case.
 - 3. Use numbers in the password.
 - 4. Use non-alphanumeric characters.
 - 5. Note: The AS400 system only allows the #, \$, _ (underscore), and @ symbols.

After three failed attempts to log in, the County systems will lock the user out until personnel from Information Systems 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.

IV. Responsibilities:

Information Systems and Human Resources have the responsibility to enforce this policy. Enforcement will be through systematic means and interaction with computer 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.

V. Support:

All Door County computer users are to contact the IS staff for support of the password

Approved March 25, 2003
County Board Resolution 33-03

Appendix C DOOR COUNTY NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Purpose of this Notice: Door County must maintain the privacy of your personal health information and give you this notice that describes our legal duties and privacy practices concerning your personal health information.

In general, when we release your health information, we must release only the information we need to achieve the purpose of the use or disclosure. However, all of your personal health information that you designate will be available for release if you sign an authorization form, if you request the information for yourself, to a provider regarding your treatment, or due to a legal requirement. We must follow the privacy practices described in this notice.

However, we reserve the right to change the privacy practices described in this notice, in accordance with the law. Changes to our privacy practices would apply to all protected health information we maintain. In the event of a change, Door County will provide a copy of the revised Notice to you upon request. Please contact the designated Privacy Officer to obtain any revised copy of the Privacy Notice.

EFFECTIVE DATE: April 14, 2003.

Uses and Disclosures of Protected Health Information (“PHI”): Door County may use PHI for the purposes of treatment, payment, and other health care operations. Examples of our use of your PHI:

1. For Treatment Purposes:

- A nurse obtains treatment information about you and records it in a health record.
- During the course of your treatment, the physician determines he/she will need to consult with another specialist in the area. He/she will share the information with such specialist and obtain his/her input.

2. For Payment Purposes:

- We submit a request for payment to your health insurance company. The health insurance company requests information from us regarding medical care given. We will provide information to them about you and the care given.

3. For Health Care Operations:

- The state licensing authority wants to review records to assure that we have acted consistent with state law regarding your care. In doing so, it wants to take a sampling that includes review of your chart. At the licensing authority’s request, we *will* provide it with a copy of your record.

4. Business Associates: We have business associates with whom we may share your PHI. For example, in preparing our annual financial statement, auditors may need to review samples of the medical care given. We may disclose your health information to the accounting firm to prepare this material.

5. Notification: Unless you object, we may use and/or disclose your PHI to notify, or assist in notifying, a family member, personal representative, or other person responsible for your care, about your location, and about your general condition, or your death.
6. To Those Involved With Your Care or Payment of Your Care: If people such as family members, relatives, or close personal friends are helping care for you or helping you pay your medical bills, we may release important health information about you to those people. The information released to those people may include your location within our facility, your general condition, or death. You have the right to object to such disclosure, unless you are unable to function or there is an emergency.
7. Disaster Relief: We may use and/or disclose your PHI to organizations authorized to handle disaster relief efforts so those who care for you can receive information about your location or health status.
8. As Required or Permitted by Law: Sometimes we must report some of your PHI to legal authorities, such as law enforcement officials, court officials, or government agencies. For example, we may have to report abuse, neglect, domestic violence or certain physical injuries, or respond to a court order.
9. Public Health Activities: We may be required to report your PHI to authorities to prevent or control disease, injury, or disability. This may include using your medical record to report certain diseases, injuries, birth or death information, information of concern to the Food and Drug Administration, or information related to child abuse or neglect. We may also have to report to your employer certain work-related illnesses and injuries so that your workplace can be monitored for safety.
10. Health Oversight Activities: We may disclose your PHI to authorities so they can monitor, investigate, inspect, discipline or license those who work in the health care system or for government benefit programs.
11. Activities Relating to Death: We may disclose your health information to coroners, medical examiners and funeral directors so they can carry out their duties related to your death, such as identifying the body, determining cause of death, or in the case of funeral directors, to carry out funeral preparation activities.
12. Organ, Eye, or Tissue Donation: Consistent with applicable law, we may disclose your PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant.
13. Research: We may disclose information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your PHI.
14. To Avoid a Serious Threat to Health or Safety: As required by law and standards of ethical conduct, we may release your PHI to the proper authorities if we believe, in good faith, that such release is necessary to prevent or minimize a serious and approaching threat to your or the public's health or safety.

15. For Military, National Security, or Incarceration/Law Enforcement Custody: If you are involved with the military, national security or intelligence activities, or you are in the custody of law enforcement officials or an inmate in a correctional institution, we may release your PHI to the proper authorities so they may carry out their duties under the law.
16. For Workers' Compensation: We may disclose your PHI to the appropriate persons in order to comply with the laws related to workers' compensation or other similar programs. These programs may provide benefits for work-related injuries or illness.
17. Judicial Proceedings: We may disclose your PHI in the course of any judicial or administrative proceeding as allowed or required by law, with your consent, or as directed by a proper court order.

Any other use or disclosure of PHI, other than those listed above, will only be made with your written consent or an authorization (an authorization specifically identifies the information we seek to use or disclose, as well as when and how we seek to use or disclose it). You may revoke your consent or authorization at any time, in writing, except to the extent that we have already used or disclosed medical information in reliance on that consent or authorization.

Your Health Information Rights: You have several rights with regard to your PHI. Specifically, you have the right to:

1. Inspect and Copy Your PHI. With a few exceptions, you have the right to inspect and obtain a copy of your health information. However, this right does not apply to psychotherapy notes or information gathered for judicial proceedings. We may also charge you a reasonable fee for you to copy any medical information that you have the right to access. In limited circumstances, we may deny you access to your PHI, and certain types of denials may be appealed. We have available forms to request PHI and will provide a written response if we deny you access and let you know your appeal rights. If you wish to inspect and copy your medical information, you should contact the privacy officer listed at the end of this Notice.
2. Request to Correct Your PHI. If you believe your PHI is incorrect, you may ask us to correct the information. You are asked to make such requests in writing and to give a reason as to why your PHI should be changed. A proper form will be provided to you upon your request. We are permitted by law to deny your request to amend your PHI if we did not create the health information that you believe is incorrect, or if we disagree with you and believe your health information is correct. You may file a statement of disagreement if your amendment is denied, and require that the request for amendment and any denial be attached in all future disclosures of your PHI.
3. Request Restrictions on Certain Uses and Disclosures. You have the right to ask for restrictions on how your health information is used or to whom your information is disclosed, even if the restriction affects your treatment or our payment or health care operation activities. Or you may want to limit the health information provided to family or friends involved in your care or payment of medical bills. You may also want to limit the health information provided to authorities involved with disaster relief efforts. Any request for restriction on certain uses and disclosures of your PHI shall be done by submitting the request in writing to Richard Burress @ 319 S. 18th Ave. Sturgeon Bay, WI 54235. We are not required to agree to any restrictions you request, but we will comply with any request granted.

4. Request an Accounting of Our Use and Disclosures of your PHI. You may request an accounting from us a list of certain disclosures of your PHI that we have made in the last six (6) years prior to the date of your request. We are not required to give you an accounting of information we have used or disclosed for purposes of treatment, payment or health care operations, or of uses or disclosures made prior to April 14, 2003. This list must include the date of each disclosure, who received the disclosed health information, a brief description of the health information disclosed, and why the disclosure was made. We must comply with your request within sixty (60) days, unless you agree to a thirty (30) day extension, and we may not charge you for the list, unless you request such list more than once per year. An accounting will not include internal uses of information for treatment, payment or health care operations, disclosures made to you or made at your request, or disclosures made to family members or friends in the course of providing care. In addition, we will not include in the list disclosures made for our directory, national security, law enforcement/corrections, and certain health oversight activities. If you wish to request an accounting of the medical information about you that we have used or disclosed, you should contact the privacy officer listed at the end of this Notice.
5. Request Communications of PHI in Alternative Means or Locations. You have the right to request that we communicate you PHI to you in different ways or places. For example, you may wish to receive information about your health status in a special, private room or through a written letter sent to a private address. We are required to accommodate reasonable requests.
6. Obtain a Paper copy of This Notice. Upon your request, you may at any time obtain a paper copy of the Notice of Privacy Practices for PHI by making a request at Emergency Services of Door County @ 319 S. 18th Ave., Sturgeon Bay, WI 54235, even if you earlier agreed to receive this notice electronically. In addition, this Notice will be available on our website that provides information about our entity. The address of our website is rburress@co.door.wi.us.
7. Legal Rights and Complaints. Notice of any changes in the Privacy Policy may be shown directly on the consent form and this Notice will be updated when any significant changes in our privacy practices occur. Emergency Services of Door County reserves the right to change the terms of this Notice at any time and the changes will be effective immediately. We also reserve the right to make any changes effective for PHI that we have created or received prior to the effective date of the Notice provision that was changed.

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the federal Department of Health and Human Services. You will not be retaliated against in any way for filing such a complaint. To file a complaint with either entity, please contact Richard Burress @ 319 S. 18th Ave., Sturgeon Bay WI 54235, who will provide you with the necessary assistance and paperwork.

Should you have any questions, comments, or complaints you are requested to direct all inquiries to the privacy officer listed at the end of this Notice.

Grant Thomas, Door County Corporation Counsel
421 Nebraska St.
Sturgeon Bay, WI 54235
920-746-2371

Appendix D

Patient Signature on file for requirement of HIPAA

I have received, from a Door County Emergency Medic, information on my rights to privacy (HIPAA).

Patient/family of patient signature

Date

Rights to privacy documents have been given to:

Patient/family of patient

Date

The patient is unable to sign due to their illness or injury.

Medic

Date

Forms/EMS/medicare sig card