

WAUSHARA COUNTY SYSTEM ACCESS POLICY

Table of Contents

Policy.....	1
Key Definitions	1
Procedures	2
1. Access Establishment and Modification.....	2
2. Workforce Clearance Procedures	3
3. Access Authorization	3
4. Person or Entity Authentication	3
5. Unique User Identification.....	3
6. Password Management	4
7. Automatic Access Limitations	4
8. Workstation Use	5
9. Workstation Security.....	5
10. Smart Phone Use	6
11. Termination Procedures.....	7
Appendix 1: Confidentiality and Information Access Agreement.....	8

Policy

It is the policy of Waushara County to safeguard the confidentiality, integrity and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. Access to information systems to all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of Waushara County's information systems. The same levels of confidentiality that exist for hard copy PHI, business and proprietary information apply to digital and/or electronic protected health information (ePHI) with Waushara County's information systems and are extended even after termination or other conclusion of access.

Key Definitions

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Minimum Necessary Information: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The "minimum necessary" standard applies to all protected health information in any form.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual
- The provision of health care to an individual
- The past, present or future payment for the provision of health care to an individual

Role: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.

Workforce: As defined in the HIPAA Privacy Rule: employees, volunteers (board members, community representatives), trainees, students, contractors and other persons under the direct control of a covered entity.

Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), *BlackBerries*, tablet PCs and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware (i.e. Ethernet ports, hard drive, etc.), operating systems, application software and network connections (including remote and wireless).

Procedures

1) Access Establishment and Modification (164.308a4iiC)

- A) All requests for access to any of Waushara County’s information systems and applications must be accompanied by a “Confidentiality and Information Access Agreement” form (see Appendix 1) completed by the intended user and approved by the user’s immediate supervisor, Department Head or Administrative Coordinator.
 - i) Access will not be granted until receipt, review and approval of a signed “Confidentiality and Information Access Agreement” form.
 - ii) The “Confidentiality and Information Access Agreement” form will be maintained by the Data Processing Department.
- B) The Department Head is responsible for notifying Data Processing of employees transferring into a new department or new role when access required is to change.
 - i) Data Processing is responsible for changing the user’s access to information systems based on the employee’s new role within 24 hours of notification or as soon thereafter as is reasonably possible.

2) Workforce Clearance Procedures (164.308a3iiB)

- A) The level of security assigned to a user to Waushara County's information systems is based on the minimum necessary 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 carry out treatment, payment or healthcare operations.
- B) All access requests are treated on a "least-access principle"; blanket access will not be provided for any user.

3) Access Authorization (164.308a4iiB)

- A) Role based categories for each information system/application are pre-approved by the Security Officer, Privacy Officer, Administrative Coordinator and Department Head. Categories are defined by the importance of the applications running on the information system, value or sensitivity of the ePHI 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.
- B) Data Processing will grant the level of access to users based on these pre-determined categories.

4) Person or Entity Authentication (164.312d)

- A) 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 (164.312a2I)

- A) Access to Waushara County's information systems/applications is controlled by requiring unique User Login Id's and passwords for each individual user.
- B) Passwords will be assigned by the Data Processing Department at the time that User Login Id is created and assigned.
- C) Passwords will not be displayed at any time. Password characters are replaced with asterisks "*" when typed.
- D) Users may not change their assigned password.

6) Password Management (164.308a5iiD)

- A) User Login Ids and passwords are used to control access to Waushara County's information systems and may not be disclosed to anyone for any reason.
- B) 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.
- C) The only people who will know the User Login Ids and passwords will be the individual user and the Security Officer.
- D) The information systems will be programmed to deny a user's ability to use without a User Login Id and password.
- E) Users that do not remember their User Login Id and/or password may contact the Security Officer. The Security Officer shall provide the user with a Login Id and password.
- F) User Login Id's and passwords will be inactivated immediately upon an employee's termination.
- G) If a user believes that his/her User Login Id or password has been compromised, he/she must report the incident to the Security Officer and his/her supervisor immediately.

7) Automatic Access Limitations (164.312a2iii)

- A) Users are required to make information systems inaccessible by any other individual when unattended by the user (i.e. using a password protected screen saver or logging off the system)
- B) Users must log off information systems/applications at the end of their shift or at the end of their need to use the system/application, whichever is sooner.
- C) Information systems will automatically go to a password protected screen saver after 15 minutes of inactivity.
- D) Exceptions to automatic log off requirements must be pre-approved by the Security Officer and Privacy Officer.

8) Workstation Use (164.310b)

- A) Waushara County's workstations may only be used for authorized business purposes.

- B) Workstations shall be placed in secure areas away from regular client traffic and display screens shall be positioned to minimize unauthorized viewing and/or access.
- C) All users are responsible for practicing precautions to protect the confidentiality, integrity and availability of ePHI in information systems at all times.
- D) Workstations may not be used to engage in any activity that is illegal or is in violation of Waushara County policies, including but not limited to the Network, Internet and E-mail Procedures and Article 6, Discipline Q) of the Waushara County Personnel Policies.
- E) Messages sent and received will be randomly monitored for compliance by the Corporation Counsel.

9) Workstation Security (164.310c)

- A) Workstations are the property of Waushara County and must always remain on premises, unless the Security Officer and/or Department Head has given prior authorization for removal.
- B) Workstations utilized off Waushara County premises are protected with security controls equivalent to those for on-site workstations.
- C) Users may only access and utilize workstations as assigned by their Department Head and/or supervisor.
- D) Department Heads and/or their designee are responsible for monitoring use of workstations.
- E) All users must report unauthorized workstation use to their Department Head/Supervisor and/or the Security Officer.
 - i. Department Heads and the Security Officer will communicate to ensure that each is aware of the unauthorized use.
- F) Waushara County will install on all workstations anti-virus software to prevent the transmission of malicious software. This software will be regularly updated.
- G) Portable workstations will also be subject to the same safeguards and protections. Users shall maintain portable workstations in a safe and secure manner when transporting.
- H) Networks are secured with a Firewall.

- i. Network access is limited to legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the Waushara County secure network.
 - ii. Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment.
 - iii. The configuration of firewalls used to protect networks are approved by the Security Officer and maintained by the Data Processing Department.
- l) Servers are located in a physically secure environment and are on a secure network with firewall protection.
- i. The system administrator or root account is password protected.
 - ii. All unused or unnecessary services are disabled.

10) Smart Phone Use

Waushara County has chosen to provide BlackBerry devices and infrastructure for use by county employees authorized by the appropriate Department Manager. BlackBerry devices are subject to the following:

A) Remote access to the county email by any means is subject to the existing Network Policy.

B) Any **county** computer resource, whether a physical device or electronic data, is county property.

C) It is the responsibility of the employee using a county BlackBerry device to maintain the appropriate security and confidentiality of the county device.

D) Use of a personal BlackBerry device to store and access county resources may subject the device or information stored on that device to audit by management, public disclosure, and/or a legal discovery process.

E) Expenses will be charged back to the departments using the BlackBerry services.

F) Only the base BlackBerry operating system and default applications will be supported.

G) The departments using county BlackBerry devices are responsible for keeping track of said devices.

H) Employees must have permission from Department Manager to use personal BlackBerries for county business.

11) Termination Procedures (164.308a3iiC)

- A) Administration and/or Department Heads/Supervisors are required to notify Data Processing when a user's employment with Waushara County has terminated.
- B) The Department Head is required to report to Administration and/or Corporation Counsel to request a termination in a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report that is filed with the Privacy Officer):
 - i. The user has been using their access rights inappropriately
 - ii. 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)
 - iii. An unauthorized individual is utilizing a user's Login Id and/or 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/or password)
- C) The Data Processing Department will terminate a user's access rights immediately upon notification.
- D) The Data Processing Department will audit and may terminate access of users that have not logged into Waushara County's information systems/applications for a period of over six (6) months.
- E) Accounts and their contents may be deleted from Waushara County system by the Data Processing Department when the account is terminated upon the Data Processing Coordinator receiving verification from Administration and/or the Corporation Counsel that the information in the accounts is no longer needed.

Effective Date: 2/9/10

Signed By: /s/ Norman Weiss
Norman Weiss, County Board Chair

Appendix 1. Confidentiality and Information Access Agreement

Summary

Waushara County is dedicated to safeguarding and maintaining the confidentiality, integrity, and availability of our client, employee, and organizational information (collectively “Confidential Information”). Client information includes protected health information that is any personal, employment-related, or medical information relating to a patient’s treatment, payment, or health care operations of Waushara County as determined through observation, conversation with a client or other medical staff, and/or information which is created and/or stored in any information system. The confidentiality, integrity, and availability of protected health information must be maintained at all times.

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

1. 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.	8. I understand that access to all Waushara County Information Systems including Email and Internet are intended for business usage.
2. 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. Protected health information is specifically protected, by law, from further disclosures without prior authorization.	9. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved privacy and security standards.
3. I will not access my own, or my family’s, record in any information system without prior Authorization (unless required to perform your job responsibilities).	10. I will only access or use the systems or devices that I am being authorized to access and agree not to demonstrate the operation or function of any of Waushara County information systems or devices to unauthorized individuals.
4. I will not disclose any Confidential Information with others who do not have a need to know it.	11. I will never use tools or techniques to break/exploit security measures.
5. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.	12. I will never connect to unauthorized networks through Waushara County systems or devices.
6. I will not download any Confidential Information off Waushara County information systems to store or use it on any other system or computer diskettes, compact discs, digital video discs, zip discs, other portable media, etc. or removable storage devices such as removable USB flash discs, except in situations whereby explicit approval to do so has been granted by Waushara County Data Processing with prior review by my Department Head, the Technical Security Officer & 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.	13. I understand that I have neither ownership interest nor expectation of privacy in any information accessed or created by me during my relationship with Waushara County. Waushara 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, security, and availability of Confidential Information.
7. I will not download any software program onto Waushara County equipment without prior written approval from the Data Processing Department.	14. I will not use Waushara County information systems to transmit, retrieve, nor store any communications consisting of discriminatory, harassing, obscene, solicitation, or criminal information.

<p>15. I understand that my User Login ID(s), password(s) are used to control access to Waushara County XYZ information systems and an electronic signature(s) is the equivalent to my legal signature. I will not disclose them to anyone nor allow anyone to access any information system using my User Login ID(s) and password(s) for any reason.</p>	<p>19. I will immediately report to the Data Processing Coordinator and/or my Department Head any activity that violates this agreement, Confidential Information laws, or any other incident that could have any adverse impact on Confidential Information.</p>
<p>16. I understand that I will be held accountable for all inquires, entries, and changes made to any Waushara County information system using my User Login ID(s) and password(s).</p>	<p>20. Upon completion and/or termination of access to Waushara County information systems, Administration and/or Department Heads/Supervisors notifies the Data Processing Department to delete Users access to information systems/applications; Department directors notify for non-workforce members.</p>
<p>17. I will only use my officially assigned, personal User Login ID(s) and password(s).</p>	<p>21. I affirm that I will maintain the confidentiality, integrity, and availability of all Confidential Information even after termination, completion, cancellation, expiration, or other conclusion of access to Waushara County information systems.</p>
<p>18. I will immediately notify the Security Officer and my immediate supervisor if my password has been seen, disclosed, or otherwise compromised.</p>	<p>22. 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 Waushara County as well as legal actions.</p>

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

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it. The Data Processing Department may deny access to Waushara County information systems if this Agreement is not returned signed and dated.

Signature

Date

Requestor's Immediate Supervisor Signature

Date

Access Agreement Approved by (printed name)

Date

Please return this completed Agreement to: Privacy Officer.