

# **Cedar County**

## **Privacy Policies & Procedures**

### **Health Insurance Portability and Accountability**

#### **Act of 1996 "HIPAA"**

#### ***Security Policies and Procedures Amendment***

**Table of Contents**

1. HIPAA Compliance Dates
2. Documentation Requirements - §164.316
3. General Security Compliance Policy #1 - §164.306
4. Administrative Safeguards - §164.308
5. Physical Safeguards - §164.310
6. Technical Safeguards - §164.312
7. Administrative Safeguards Security Management Policy #2 - §164.308(a)(1)
8. Administrative Assigned Security Responsibility Policy #3 - §164.308(a)(2)
9. Administrative Safeguards Workforce Security Policy #4 - §164.308(a)(3)
10. Administrative Safeguards Information Access Management #5 - §164.308(a)(4)
11. Administrative Safeguards Security Awareness and Training #6 - §164.308(a)(5)
12. Administrative Safeguards Incident Response and Reporting Policy #7 - §164.308(a)(6)
13. Administrative Safeguards Contingency Plan Policy #8 - §164.308(a)(7)
14. Periodic Evaluation of Security Policies and Procedures Policy #9 - §164.308(a)(8)
15. Administrative Safeguards Business Contacts and other Arrangements #10 - §164.308(b)(8)
16. Physical Safeguards Facility Access Controls Policy #11 - §164.310(a)(1) & (2)
17. Physical Safeguards Workstation Use Policy #12 - §164.310(b)
18. Physical Safeguards Server, Desktop and Wireless Computer System Security Policy #13 - §164.310(c)
19. Physical Safeguards Device and Media Controls Policy #14 - §164.310(d)(1) & (2)
20. Technical Safeguards Access Controls Policy #15 - §164.312(a)(1) & (2)
21. Technical Safeguards Audit Controls Policy #16 - §164.312(b)
22. Technical Safeguards EPHI Integrity Policy #17 - §14.312(c)(1) & (2)
23. Technical Safeguards Person or Entity Authentication Policy #18 - §164.312(d)
24. Technical Safeguards Transmission Security Policy #19 - §164.312(e)(1) & (2)

**Compliance Dates  
HIPAA SECURITY**

**Compliance Dates for the Initial Implementation of the Security Standards §164.318**

A health plan that is not a small health plan must comply with the applicable requirements no later than April 20, 2005.

A small health plan must comply with the applicable requirements no later than April 20, 2006.

A health care clearinghouse must comply with the applicable requirements no later than April 20, 2005.

**A County that is a covered health care provider must comply with the applicable requirements no later than April 20, 2005.**

**Security Policies and Procedures**

The Cedar County HIPAA Security Policies and Security Procedures are designed to ensure compliance with the Security Regulations. Such Security Policies and Security Procedures shall be kept current and in compliance with any changes in the law, regulations or practices of Cedar County's covered entity component parts in accordance with HIPAA Security Regulations.

## Documentation Requirements

### **Policies and Procedures §164.316(a)**

The County will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications or other requirements of the HIPAA regulation. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification or other requirements of the HIPAA regulation.

The County may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the HIPAA regulation.

### **Documentation §164.316(b)(1)**

The County will maintain the policies and procedures implemented to comply with the HIPAA regulation (which may be electronic form); and if an action, activity or assessment is required by the HIPAA regulation to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.

### **Time limit (Required) §164.316(b)(2)(i)**

The County will retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

### **Availability (Required) §164.316(b)(2)(ii)**

The County will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

### **Updates (Required) §164.316(b)(2)(iii)**

The County will review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information (PHI).

## General Requirements

### General Requirements §164.306(a)

The County will do the following:

1. Ensure the confidentiality, integrity and the availability of all electronic protected health information (PHI) the County creates, receives, maintains or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required..
4. Ensure compliance with the security standards identified in the HIPAA regulations.

### Flexibility §164.306(b)

1. The County may use any security measures that allow the County to reasonably and appropriately implement the standards and implementation specifications as specified in the security standards of HIPAA.
2. In deciding which security measures to use, the County will take into account the following factors:
  - a. The size, complexity and capabilities of the County.
  - b. The County's technical infrastructure, hardware and software security capabilities.
  - c. The costs of security measures.
  - d. The probability and criticality of potential risks to protected health information.

### Standards §164.306(c)

The County will comply with the standards of the HIPAA security regulations with respect to all PHI.

### Implementation Specifications §164.306(d)

Implementation specifications are either required or addressable. When "required" appears in parentheses after the title of a implementation specification the County will implement the implementation specification. When "addressable" appears in parentheses after the title of an implementation specification the County will assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the County's electronic PHI.

If the implementation specification is reasonable and appropriate the County will implement the specification. If the implementation specification is not reasonable and appropriate the County will:

- a. document why it would not be reasonable and appropriate to implement the implementation specification; and
- b. the County will implement an equivalent alternative measure if reasonable and appropriate.

### Maintenance §164.306(e)

The County will review and modify security measures implemented to comply with the HIPAA regulation to continue reasonable and appropriate protection of electronic PHI.

## **Administrative Safeguards**

### **Security Management Process (Required) §164.308(1)(i)**

The County will implement policies and procedures to prevent, detect, contain and correct security violations.

### **Risk Analysis (Required) §164.308(1)(ii)(A)**

The County will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (PHI) held by the County.

### **Risk Management (Required) §164.308(1)(ii)(B)**

The County will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

### **Sanction Policy (Required) §164.308(1)(ii)(C)**

The County will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the County.

### **Information System Activity Review (Required) §164.308(1)(ii)(D)**

The County will implement procedures to regularly review records of information activity, such as audit logs, access reports and security incident tracking reports.

### **Assigned Security Responsibility (Required) §164.308(2)**

The County will identify the security official who is responsible for the development and implementation of the policies and procedures.

### **Workforce Security (Required) §164.308(3)(i)**

The County will implement policies and procedures to ensure all members of the workforce have appropriate access to electronic PHI and to prevent those workforce members who do not need access from obtaining access to electronic PHI.

### **Implementation Specifications §164.308(3)(ii)**

#### **1. Authorization and/or Supervision (Addressable)**

The County will implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.

#### **2. Workforce Clearance Procedure (Addressable)**

The County will implement procedures to determine that the access of a workforce member to electronic PHI is appropriate

#### **3. Termination Procedures (Addressable)**

The County will implement procedures for terminating access to electronic PHI when the employment of a workforce member ends.

### **Information Access Management (Required) §164.308(4)(i)**

The County will implement policies and procedures for authorizing access to electronic PHI that are consistent with the HIPAA regulation.

### **Implementation Specifications §164.308(4)(ii)(A)**

#### **1. Health Care Clearinghouse Functions. (Required)**

If the County is a health care clearinghouse that is part of a larger organization, the County clearinghouse must implement policies and procedures that protect the electronic PHI of the County clearinghouse from unauthorized access by the larger organization.

**2. Access Authorization. (Addressable)**

The County will implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process or other mechanism.

**3. Access Establishment and Modification. (Addressable)**

The County will implement policies and procedures that, based upon the County's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program, or process.

**Security Awareness and Training §164.308(5)(i)**

The County will implement a security awareness and training program for all members of its workforce including management.

**Implementation Specifications §164.308(5)(ii)**

1. The County will implement:

**a. Security Reminders. (Addressable)**

Periodic security updates.

**b. Protection from Malicious Software. (Addressable)**

Procedures for guarding against, detecting and reporting malicious software.

**c. Log-in Monitoring. (Addressable)**

Procedures for monitoring log-in attempts and reporting discrepancies.

**d. Password Management. (Addressable)**

Procedures for creating, changing and safeguarding passwords.

**Security Incident Procedures §164.308(6)(i)**

The County will implement policies and procedures to address security incidents.

**Response and Reporting (Required) §164.308(6)(ii)**

The county will Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the County; and document security incidents and their outcomes.

**Contingency Plan §164.308(7)(i)**

The County will establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI.

**Implementation Specifications §164.308(7)(ii)****1. Data Backup Plan. (Required)**

The County will establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.

**2. Disaster Recovery Plan. (Required)**

The County will establish (and implement as needed) procedures to restore any loss of data.

**3. Emergency Mode Operation Plan. (Required)**

The County will establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.

**4. Testing and Revision Procedures. (Addressable)**

The County will implement procedures for periodic testing and revision of contingency plans.

**5. Applications and Data Criticality Analysis. (Addressable)**

The County will assess the relative criticality of specific applications and data in support of other contingency plan components.

**Evaluation (Required) §164.308(8)**

Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI, that establishes the extent to which the County's security policies and procedures meet the requirements of the HIPAA regulation.

**Business Associate Contracts and Other Arrangements (Required) §164.308(8)(b)(1)**

A County, in accordance with §164.306, may permit a Business Associate to create, receive, maintain or transmit electronic PHI on the County's behalf only if the County obtains satisfactory assurances, in accordance with §164.314(a) that the Business Associate will appropriately safeguard the information.

This standard does not apply with respect to:

- a. The transmission by the County of electronic PHI to a health care provider concerning the treatment of in individual.
- b. The transmission of electronic PHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and §164.504(f) apply and are met; or
- c. The transmission of electronic PHI from or to other agencies providing the services at §164.502(e)(1)(ii)(C), when the County is a health plan that is a government program providing public benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.

If the County violates the satisfactory assurances it provided as a business associate of another covered entity the County will be in noncompliance with the standards, implementation specifications, and requirements of the HIPAA regulation.

**Written Contract or Other Arrangement (Required) §164.308(8)(4)**

The County will document the satisfactory assurances through a written contract or other arrangement with the business associate.

## **Physical Safeguards**

### **County Access Controls §164.310(a)(1)**

The County will implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

### **Contingency operations (Addressable) §164.310(a)(2)(i)**

The County will establish (and implement as needed) procedures that allow departmental access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

### **County Security Plan (Addressable) §164.310(a)(2)(ii)**

The County will implement policies and procedures to safeguard departments and the equipment therein from unauthorized physical access, tampering and theft.

### **Access Control and Validation Procedures (Addressable) §164.310(a)(2)(iii)**

The County will implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

### **Maintenance Records (Addressable) §164.310(a)(2)(iv)**

The County will implement policies and procedures to document repairs and modifications to the physical components of a department which are related to security (for example, hardware, walls, doors, and locks).

### **Workstation Use §164.310(b)**

The County will implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information (PHI).

### **Workstation Security §164.310(c)**

The County will implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.

### **Device and Media Controls §164.310(d)(i)**

The County will implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a department, and the movement of these items within the department.

### **Disposal (Required) §164.310(d)(2)(i)**

The County will implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.

### **Media re-use (Required) §164.310(d)(2)(ii)**

The County will implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

### **Accountability (Addressable) §164.310(d)(2)(iii)**

The County will maintain a record of the movements, hardware and electronic media and any person responsible therefore.

**Data Backup and Storage (Addressable) §164.310(d)(2)(iv)**

The County will create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

## Technical Safeguards

### **Access Control §164.312(a)(1)**

The County will implement technical policies and procedures for electronic information systems that maintain electronic protected health information (PHI) to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

### **Unique User Identification (Required) §164.312(a)(2)(i)**

The County will assign a unique name and/or number for identifying and tracking user identity.

### **Emergency Access Procedure (Required) §164.312(a)(2)(ii)**

The County will establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.

### **Automatic Logoff (Addressable) §164.312(a)(2)(iii)**

The County will implement electronic procedures that terminate an electronic session after predetermined time of inactivity.

### **Encryption and Decryption (Addressable) §164.312(a)(2)(iv)**

The County will implement a mechanism to encrypt and decrypt electronic PHI.

### **Audit Controls §164.312(b)**

The County will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

### **Integrity §164.312(c)(1)**

The County will implement policies and procedures to protect electronic PHI from improper alteration or destruction.

### **Mechanism to Authenticate Electronic Protected Health Information (Addressable) §164.312(c)(2)**

The County will implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

### **Person or Entity Authentication §164.312(d)**

The County will implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

### **Transmission Security §164.312(e)(1)**

The County will implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

### **Integrity controls (Addressable) §164.312(e)(2)(i)**

The County will implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

### **Encryption (Addressable) §164.312(e)(2)(ii)**

The County will implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

**General Security Compliance Policy  
HIPAA Security Policy #1**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Policy covers Cedar County's approach to compliance with the Security Regulations. Cedar County will:

1. designate a Security Compliance Officer.
2. ensure the confidentiality, integrity and availability of all PHI Cedar County creates, receives, maintains or transmits
3. protect against any reasonably anticipated threats or hazards to the security or integrity of such information
4. protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
5. ensure compliance with the Security Regulations by its Workforce.

PROCEDURE

**1) Security Personnel and Implementation**

Cedar County has designated a Security Officer with overall responsibility for the development and implementation of policies and procedures for the Security Regulations.

**2) Security Complaints**

(See page 62 [Compliance Violations] of the Cedar County Privacy Policies & Procedures, First Revision, Effective October 2, 2003)

**3) Sanctions and Non-Retaliation**

(See page 62 [Compliance Violations] of the Cedar County Privacy Policies & Procedures, First Revision, Effective October 2, 2003)

**4) Responsibility of All Employees to comply with the Health Insurance Portability and Accountability Act of 1996**

(See page 59 [Workforce Confidentiality] of the Cedar County Privacy Policies & Procedures, First Revision, Effective October 2, 2003)

**5) Violations**

(See page 59 [Workforce Confidentiality] of the Cedar County Privacy Policies & Procedures, First Revision, Effective October 2, 2003)

**Hybrid Entity Component Parts**

(See Page 66 of the Cedar County Privacy Policies & Procedures, First Revision, Effective October 2, 2003)

**Security Management Policy  
HIPAA Security Policy #2**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to ensure that security violations are prevented, detected, contained and corrected in accordance with the Security Regulations. This Policy covers risk analysis, the security measures and safeguards, and information systems review for PHI.

PROCEDURE

**1. Risk Analysis**

- a. Cedar County acknowledges the potential vulnerabilities associated with storing PHI and transmitting PHI inside and outside the County.
- b. Cedar County will assess such potential vulnerabilities by:
  - Identify and document all PHI repositories
  - Periodically re-inventory PHI repositories
  - Identify the potential vulnerabilities to each repository
- c. Cedar County will update its PHI inventory annually.
- d. Each repository will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of contained PHI.
- e. Cedar County will reassess the potential risks and vulnerabilities to the integrity, confidentiality, and availability of each repository and the level of risk assigned to each repository at least annually.

**2. Risk Management**

- a. Cedar County will implement security measures and safeguards that are reasonable and appropriate for each PHI repository sufficient to reduce risks and vulnerabilities. Cedar County will meet the following minimum guideline in implementing security measures and safeguards:
  - Repositories will be appropriately safeguarded by normal best-practice security measures in place such as user accounts, passwords, security groups and perimeter firewalls.
- b. Cedar County will reassess the potential risks and vulnerabilities of PHI repositories as part of a periodic review and update the security measures and safeguards.
- c. Cedar County's entire Workforce is subject to compliance with the Cedar County Information Security Policy. Where PHI is involved, the HIPAA Security Policies supersede any Cedar County Information Security Policy.
- d. The security measures and safeguards implemented for each PHI repository will be documented by the HIPAA Security Officers.

**3. Sanctions for Noncompliance**

- a. To ensure that all members of the Workforce fully comply with the Cedar County Security Policies, Cedar County will appropriately discipline and sanction employees and other Workforce members for any violation of the HIPAA Security Policies in accordance with the Cedar County HIPAA Privacy Policy – Privacy Compliance.

**4. Information System Activity Review**

- a. HIPAA Security Officer will audit IT AS400 logs monthly for journaling and random checks for inappropriate entry.
- b. Information to be audited will include date, time, person logging in, and records accessed.
- c. HIPAA Security Officer will inspect Security incident log monthly and recommend appropriate action. Security incidents will include unauthorized access attempts, denial of service attempts, and successful virus/worm attacks.
- d. HIPAA Security Officer will take appropriate action to insure repair of weaknesses and violations.
- e. In conjunction with HIPAA Security Officer, Department Heads will insure that passwords are changed, backups are performed, and department PCs are secured.

**Assigned Security Responsibility Policy  
HIPAA Security Policy #3**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Policy covers the procedures for identifying the security official who is responsible for the development and implementation of the policies and procedures for HIPAA Security.

PROCEDURE

Cedar County will assign and document the persons who are responsible for the development and implementation of the policies and procedures for HIPAA Security:

ASSIGNMENTS

Compliance/Privacy Officer: Rob Young  
Phone: 563-886-2170  
E-Mail: ryoung@cedarcountry.org

Security Officer: Bev Penningroth  
Phone: 563-886-3168  
E-Mail: bpenningroth@cedarcountry.org

Deputy Security Officer: Rick Fleshin  
Phone: 563-886-2226  
E-Mail: rfleshin@cedarcountry.org

Contact Office: Board of Supervisors  
Phone: 563-886-3168  
E-Mail: bos@cedarcountry.org

**Workforce Security Policy  
HIPAA Security Policy #4**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to ensure that all Workforce members have appropriate access to PHI and to prevent Workforce members who do not have access to PHI from obtaining such access. This Policy covers the procedures Cedar County has implemented to ensure that access to PHI is authorized, supervised and appropriate, and procedures to terminate access if not necessary.

**Authorization and/or Supervision of PHI**

Cedar County will create procedures to ensure that only users with a need to access PHI are granted access to PHI.

**Workforce Clearance Procedure**

Cedar County will create procedures to determine that the access to PHI is needed and appropriate for each user.

**Termination of Access**

Cedar County will develop and implement a procedure for terminating access to PHI when the user's employment ends. This policy will be used in all terminations of employee's and when access to PHI is no longer needed.

PROCEDURE

**Authorization and/or Supervision of PHI**

Any user needing access to PHI must be approved through their supervisor and department head before being granted access to the PHI. Departments will maintain documentation supporting each users access to all PHI involved. This access will be reviewed on an annual basis. Supervision will be provided for these users so unauthorized access to the PHI is avoided.

**Workforce Clearance Procedure & Termination of Access**

Users should not access PHI unless authorized by their Department Head. Department Heads should submit to Information Services documentation of the users that need access to PHI, what system the user needs access to, and what information needs to be accessed by the user. The department head, department head's designee, or Information Services Director, would then be allowed to set up a user account and password on a PC. If a user account and password is needed for the user to access the IBM AS400 computer, the Information Services Director will set up the user profile. When a user's employment ends with Cedar County, the department head should notify Information Services, at which time the user's profile/account should be deleted from all systems. The following form could be utilized by department heads to support users' access.

**Documentation For User Access Authorization, Clearance, Termination**

**Department:**

**User:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Systems To Be Accessed:** \_\_\_\_\_

**Information To Be Accessed:**

**Date of Termination of Access:** \_\_\_\_\_

=====

**User:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Systems To Be Accessed:** \_\_\_\_\_

**Information To Be Accessed:**

**Date of Termination of Access:** \_\_\_\_\_

=====

**User:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Systems To Be Accessed:** \_\_\_\_\_

**Information To Be Accessed:**

**Date of Termination of Access:** \_\_\_\_\_

=====

**Information Access Management Policy  
HIPAA Security Policy #5**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to ensure that access to PHI is properly authorized. This Policy describes how Cedar County will ensure that access to PHI is assigned and managed.

**1. Health Care Clearinghouse Functions**

Cedar County is not a health care clearinghouse that is part of a larger organization so we have no access by a larger organization.

**2. Access Authorization**

- a. Cedar County has established procedures for granting access to PHI through a workstation, transaction, program, or process. Procedures will include the following:
  - Elected Official's or Department heads are responsible for authorizing access to systems and areas containing PHI for his or her subordinates.
  - Access granted will be the minimum necessary access required for each job role and responsibilities.
  - Information Services will be responsible for security on networks, servers and systems by establishing security to support the separation and accessibility of PHI data and programs.

**3. Access Establishment and Modification**

- a. Cedar County has established procedures based on Access authorization procedures for review and modification of a user's right of access to PHI through a workstation, transaction, program, or process. These procedures will include the following:
  - Elected Official and Departments heads are responsible for periodically reviewing access to PHI granted to each of his or her subordinates and notifying Information Services of any changes that are appropriate.
  - Departments will follow the procedures created for employment termination. Including removal of access to County facilities. See Exhibit A.
  - If an employee transfers to another department within the County the user's access to PHI within his current department will be terminated. Any new access to PHI will be granted through his or her new department head and new role and responsibilities.

See Policy #4 Above

**Security Awareness and Training Policy  
HIPAA Security Policy #6**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to provide security awareness and training for all members of its Workforce. This Policy covers security reminders, procedures for guarding against, detecting and reporting malicious software, changing and safeguarding passwords.

**1. Security Reminders**

- a. Cedar County has established procedures on how the County departments and users will be notified of periodic updates of security changes in HIPAA security policies and procedures and Cedar County's general security policies.
- b. Cedar County has established procedures on how to notify departments and users of any warnings that are issued or discovered, reported or potential threats. See Exhibit A.

**2. Protection from Malicious Software**

- a) Cedar County will provide training to all its users on how to identify and protect against malicious code and software.
- b) Information Services will develop and implement procedures to detect and guard against malicious code such as viruses, worms, ad ware, and any other computer program or code designed to interfere with normal operation of a system. See Exhibit A.
- c) A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up to date. Information Services will review any instance where virus detection software cannot be maintained on a workstation and therefore would not be practical to install, and may waive the requirement to install virus detection and ad ware software.
- d) Information Services will notify all departments and users of new and potential threats from malicious code such as viruses, worms, denial of service attacks, and any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.
- e) Departments and users must notify Information Services if a virus, worm or other malicious code has been identified.
- f) Information Systems will be responsible for ensuring that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network. See Exhibit B.

**3. Password Management**

- a) Information Services will develop and implement procedures for creating, changing, and safeguarding passwords.
- b) The following minimum password procedures will be followed:
  - All County Employees who use a computer or has access to network resources or systems will have a unique user identification and password.
  - All computers, network resources, system and applications will require the user supply a password in conjunction with their unique user identification to gain access.
  - All passwords will be of sufficient complexity to ensure that it is not easily guessable.

- Department heads will be responsible for making their employees aware of all password-related policies and procedures, and any changes to those policies and procedures.
- Information Services will be responsible for setting password aging times for systems, networks and applications. Passwords should be changed at least every 90 days.
- All Cedar County employees are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
  1. Passwords are only to be used for legitimate access to networks, systems, or applications.
  2. Passwords must not be disclosed to other users or individuals, except to department heads, as may be required.
  3. Employees must not allow other employees or individuals to use their password.
  4. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

#### 4. Security Training Program

- a) Cedar County will ensure that its Employees have been given the appropriate level of HIPAA security training so that all Employees who access, receive, transmit or otherwise use PHI are familiar with Security policies and procedures and their responsibilities regarding such policies and procedures. Training will consist of the following:

- HIPAA Security Policies
- HIPAA Business Associate Policy
- HIPAA Sanction Policy
- Confidentiality, integrity and availability
- Individual security responsibilities
- Common security threats and vulnerabilities

In addition those who set up, manage or maintain systems and workstations will receive this training;

- Password structure and management procedures
- Server, desktop computer, and mobile computer system security procedures, including security patch and update procedures and virus and malicious code procedures
- Device and media control procedures
- Incident response and reporting procedures

#### PROCEDURE

##### **Security Reminders**

The Privacy/Compliance Officer, Security Officer or Deputy Security Officer will notify department heads of any security changes in policies and procedures. Warnings regarding security may be issued to departments by email, telephone or in person. Department heads should notify users of any security changes or warnings.

##### **Malicious Software Detection and Prevention Procedure**

Department heads will assure that all systems have anti-virus software and ad ware software installed. If needed, Information Services will assist with the installation of such software. Before the software is installed, department heads should obtain the approval of Information Services. Anti-virus software should be updated daily and systems should be scanned daily. Ad ware software should be updated and executed at least weekly.

**Incident Response and Reporting Policy  
HIPAA Security Policy #7**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to address security incidents. This Policy covers how Cedar County will respond to and document security incidents.

**1. Common Incident Response and Reporting System**

Cedar County has created an Incident Response and Reporting System to report, mitigate, and document HIPAA security incidents and violations.

PROCEDURE

**2. Reporting and Responding to HIPAA Security Incidents**

All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of EPHI must be reported and responded to using the following procedures:

- a. Users will notify Information Services for issues involving viruses, worms, or malicious code, network or system related attacks, unauthorized access to PHI or system containing PHI and intrusion attempts from outside. If an incident involves PHI the user will notify their Security Liaison or department head.
- b. Information Services will investigate and recommend updates or fixes for security incidents, and then notify the Board of Supervisors.
- c. The HIPAA Security/Privacy Officer will notify the Board of Supervisors in regards to any privacy or security issues.
- d. All contact with outside authorities such as local police, FBI, media, etc. will go through the Board of Supervisors Office.

**3. Documentation of Security Incidents**

The Security Officer for Cedar County will document all security related incidents and their outcomes. Information Services will develop and implement disaster recovery reporting procedures for failures, outages, or data loss that involve EPHI systems or applications. Department Security Liaisons will develop and implement documentation for tracking and reporting security related incidents and their outcome for physical PHI within their departments.

**4. Mitigation of Known Security Incidents**

Security incidents involving Computers or the Network will be handled by Information Services by quarantining or removing the threat. Security Liaisons will be notified of viruses and other malicious software and any County-wide threats to PHI. Such notifications may be made by way of the County Email. The HIPAA Security Liaison is responsible for informing employees within the department. Security incidents involving physical copies of PHI will be handled by the Security Liaison within the department where the PHI is stored.

**Data Backups and Contingency Planning Policy  
HIPAA Security Policy #8**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to ensure that data can always be made available and protected during disasters or equipment failure. This Policy covers the procedures for safe guarding data in the event of an emergency, disaster, fire, vandalism, or system failure.

**1. Data Backup Plan**

- a. Information Services and Department Heads will establish and implement a Data Backup Plan which will allow for retrievable exact copies of all data and files on systems.
- b. The Data Backup Plan will require that all media used for the backups be stored in a physically secure location off-site, or in a secure location within the facility.  
See Exhibit A.

**2. Disaster Recovery Plan**

- a. Cedar County will create a plan to recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems in a timely manner.
- b. The Disaster Recovery Plan will include procedures to restore data from backups in the case of a disaster causing data loss.
- c. The Disaster Recovery Plan will be documented and easily available to the necessary personnel at all times.

**3. Emergency Mode Operation Plan**

- a. Cedar County will establish procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
- b. The Emergency Mode Operation Plan will be documented and easily available to the necessary personnel at all times.

**4. Testing and Revision Procedure**

- a. Data backup procedures should be tested on a periodic basis to ensure that exact copies can be retrieved.
- b. The Disaster Recovery Plan should be tested on a periodic basis to make sure systems and data can be restored or recovered.
- c. Emergency mode operation procedures should be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

**5. Applications and Data Criticality Analysis**

- a. Cedar County will assess the relative criticality of specific applications and data in support of other contingency plan components.

PROCEDURE

**Backup Plan**

**Overview**

The goal of backups is to prevent the loss of data in the case of system failure or the accidental deletion of data. Backups are not meant to archive data for future reference. Data stored locally on desktop computers is not backed up by Information Services nor is it backed up if it is stored on systems that are not managed by the Information Services Department.

**Procedure-AS400**

On, or about the first day of the month, a monthly backup will be done of the IBM AS400 computer.

There will be a two-week cycle of tapes. The most current week's cycle should be kept in the lock box at the bank. The most current monthly tape will be kept in the lock box at the bank. End of fiscal year and end of calendar year tapes will be kept for a period of three years in the County's fire-resistant safe.

**Verification**

Test restores from backup tapes should be performed on a periodic basis. This ensures that both the tapes and the backup procedures work properly.

**Restore Requests**

Requests to restore data on the AS400 should go through the Information Services Department.

**Procedure-Servers/Desktop Computers**

PHI on servers/desktop computers should be backed up at least weekly and stored off-site in a secure location or in a secure location within the facility. Test restores should be performed on a periodic basis. Requests to restore data on desktop computers should go through the Department Heads. Appropriate review/inspection of backup records will be held by the Information Systems Director.

**Periodic Evaluation of Security Policies and Procedures Policy  
HIPAA Security Policy #9**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This policy is to ensure that a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI is performed and to make sure Cedar County's security policies and procedures meet the requirements of the HIPAA regulation. This Policy covers the procedures to ensure that the Security Policies are periodically evaluated.

PROCEDURE

**1. Periodic Evaluation**

- a. Cedar County will evaluate its Security Policies to determine their compliance with the HIPAA Security Regulations. Cedar County will make the Security Polices compliant with the Security Regulations. Once compliant, Cedar County will evaluate its Security Policies on a periodic basis for environmental or operational changes affecting the security of PHI.
- b. The Security and Privacy Officers will on an annual basis review the Polices and Procedures Cedar County has adopted for compliance of the Security regulations.
- c. Security Liaisons for each department where PHI is available will review Security polices and procedures on an annual basis that apply to their department.
- d. When changes are made to Security Policies or Procedures all department Liaisons will be notified of the changes.
- e. Review of the Security Polices and Procedures will be made upon any changes to the HIPAA Security Regulations or Privacy Regulations.
- f. Review of the Security Polices and Procedures will be made upon a serious security violation, breach, or other security incident.
- g. Review of the Security Polices and Procedures will be made upon any change in technology, environmental processes or business processes that may affect HIPAA security.

**Business Associate Contracts and Other Arrangements Policy  
HIPAA Security Policy #10**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to ensure that access to PHI is appropriately limited. This Policy covers the procedures to allow for a Business Associate to create, receive, maintain or transmit electronic PHI on the County's behalf.

1. A County, in accordance with §164.306, may permit a Business Associate to create, receive, maintain or transmit electronic PHI on the County's behalf only if the County obtains satisfactory assurances, in accordance with §164.314(a) that the Business Associate will appropriately safeguard the information.
2. This standard does not apply with respect to:
  - a. The transmission by the County of electronic PHI to a health care provider concerning the treatment of an individual.
  - b. The transmission of electronic PHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and §164.504(f) apply and are met; or
  - c. The transmission of electronic PHI from or to other agencies providing the services at §164.502(e)(1)(ii)(C), when the County is a health plan that is a government program providing public benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.
3. If Cedar County violates the satisfactory assurances it provided as a business associate of another covered entity, the County will be in noncompliance with the standards, implementation specifications, and requirements of the HIPAA regulation.
4. Written Contract or Other Arrangement (Required) §164.308(8)(4) See Business Associate Agreement.
5. Cedar County will document the satisfactory assurances through a written contract or other arrangement with the business associate.

(See page 53-55 [Business Associate Agreements] of the Cedar County Privacy Policies & Procedures, First Revision, Effective October 2, 2003)

## **Facility Access Controls Policy HIPAA Security Policy #11**

### POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to appropriately limit physical access to PHI. This Policy covers the procedures that will limit physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

#### **Contingency Operations**

Cedar County will create procedures to allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan.

#### **County Security Plan**

Cedar County will create and maintain a general County security plan that safeguards all facilities, systems, and equipment against unauthorized physical access, tampering, and theft.

#### **Access Control and Validation Procedures**

1. Cedar County will create procedures to control and validate employee's access to facilities where PHI is available.
2. Cedar County will create and implement procedures to control, validate, and document visitor access to any facility where PHI is stored. Visitors include vendors, repair personnel, and other non-employees.
3. Cedar County will create procedures to secure the physical locations where PHI data is stored; Examples are data centers and file cabinets.
4. Facilities where PHI is available will provide appropriate access control mechanisms for access to the facility; Examples would be key lock, code lock, and badge reader.

#### **Maintenance Records**

Cedar County will create procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

### PROCEDURE

#### **Emergency Access**

Physical facility access during emergencies to support restoration of data should be authorized by the County Auditor and/or a member of the Board of Supervisors.

#### **Security Plan**

Generally, the Courthouse is unlocked from 7:45 a.m. until 4:30 p.m. The Courthouse Security Officer is responsible for unlocking and locking the facility for normal business. The Auditor's Office logs requests for use of the Courthouse for meetings during business and non-business hours, and distributes keys as-needed. Department heads are responsible for the security of their department's areas, such as locking file cabinets, doors, windows, etc. and they are responsible for locking the Courthouse doors after the conclusion of meetings, etc., which are held after normal business hours or conclude after normal business hours. Courthouse staff are responsible for the security of public areas.

**Access Control**

Employees are to wear name badges issued by the County, or other identification as required by their department heads. Distribution of keys to the facility and offices is the responsibility of the Department Heads or County Auditor. The Auditor's Office should be notified of movement of keys to new employees and current employees, for access to and within the Courthouse. Department heads are responsible for the monitoring of visitors within their work areas. A log will be kept of individuals doing repairs or working on infrastructure within the Courthouse, Law Enforcement Center or New Horizon Residential. Department heads are responsible for assuring that these individuals are logging in & out and obtaining a Visitor Tag. The log for the Courthouse will be located at the Auditor's Office. Visitors who are in areas where PHI is located, will be accompanied by County personnel.

**Maintenance Documentation**

Repairs and modifications should be documented using the form below.

**Cedar County Maintenance Reporting Form**

**Please Use this form to track all PHI affected locations and Systems. --- MAINTENANCE RECORDS §164.310 (a) (2) (iv) • Implement track and facility that include a record of when locks are changed, security systems are replaced or modified, Passwords cahnged on Sec**

Please describe briefly the Maintenance Activity that took place. If systems were involved, please list the systems affected. This may also reference a written document attached to this form.	Department Affected	Date	Seriousness Of Task			Tasks						Employee to System Affected. If System, please list Model, Serial Number and IP Address	Employee or Business Associate Assigned to this task	What Task was completed Action was tak	
			Low	Medium	High	Remodeling	Changed Locks	Changed Alarm System	Changed Employee's Pass Code	Hardware Maintenance	Software Maintenance				

**Workstation Acceptable Use Policy  
HIPAA Security Policy #12**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to outline the physical measures required to protect electronic information systems and related equipment from unauthorized use. This Policy is to specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information (PHI).

PROCEDURE

1. All Cedar County employees will comply with the Cedar County Computer and Internet Use Policy to ensure that computers that access PHI are used in a secure and legitimate manner. See Exhibit A.
2. Users of Cedar County systems and workstations should have no expectation of privacy. To appropriately manage its information systems and enforce appropriate security measures, Information Technology may log, review, or monitor any data (EPHI and non-EPHI) stored or transmitted on its information systems.
3. Cedar County may remove or deactivate any user privileges and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

## Exhibit A

### CEDAR COUNTY COMPUTER & INTERNET POLICY

The intention of providing Internet and e-mail access is intended to be for business reasons only. Cedar County encourages the use of the Internet and e-mail, it makes communication more efficient and effective; however, Internet service and e-mail are county property, and their purpose is to facilitate county business. Every staff member has a responsibility to maintain and enhance the County's public image and to use county e-mail and access the Internet in a productive manner. Any improper use of the Internet or e-mail is not acceptable and will not be permitted. To ensure that all employees are responsible, the following policy has been put in place.

#### I. PURPOSE & DESIGNATION OF INFORMATION OFFICER

The purpose of this policy is to outline Cedar County's policy for usage of Computers, Internet and Electronic Mail. The designated Information Officer is the Data Processing Systems Coordinator, as approved by the Board of Supervisors.

#### II. USAGE

- A. It is the policy of Cedar County that employees are encouraged to utilize electronic communication as an appropriate means of communication and research to improve the quality and productivity of employees.
- B. Cedar County employees are authorized to access the Internet and e-mail, however, persons having access to these tools shall utilize them in a legal, professional manner.
- C. Electronic equipment provided for the use of Cedar County employees and any work product, messages, or data transmitted through this equipment is the property of Cedar County. Users shall not download or copy data from the County computer system or any County owned computer, disk or other electronic medium onto disks or other media for personal use and no such data, disk or electronic medium shall be removed from County property.
- D. The Iowa Open Records Act (Chapter 22, Code of Iowa) and the Freedom of Information Act, as interpreted by the Courts, indicate that electronic files obtained via the Internet and E-mail communications are public records and subject to inspection by the public in the same manner as paper documents.
- E. All users should be aware that federal copyright laws may protect any information, software, or graphics on the Internet, regardless of whether a copyright notice appears on the work; Cedar County prohibits the reproduction or distribution of copyrighted information. Most software on Cedar County computers and computer systems are copyrighted and licensed to Cedar County for use in accordance with those licensing agreements. Consequently, users may not copy, reproduce or otherwise copy or download any such software or related documentation without prior approval of the Information Officer.
- F. Communications and Internet access should be conducted in a responsible and professional manner reflecting the County's commitment to honest, ethical and non-discriminatory business practice.

- G. Employees, who are terminated, laid off or on extended leave of absence have no right to the contents of their e-mail messages and are not allowed to access the computer system.
- H. Employees are warned that mere deletion of a message or file may not fully eliminate the message from the system.
- I. Cedar County employees are authorized to remove laptop computers and accessories from County facilities to utilize them for County work-related purposes. Laptop computers should be returned to County facilities as soon as possible and practical. Employees should use precautions to safeguard the computer hardware and software.

### III. CONFIDENTIALITY

- A. It is recognized that some employees may store information in their computers that is classified as confidential by law, and that information may be protected with passwords unique to individual employees. However, no passwords for screens or files may be added to the County's computer equipment without the approval of the Information Officer.
- B. Information which is protected from inspection by the public is subject to inspection by the Department Head or Information Officer.
- C. It is the responsibility of employees having custody of records classified as confidential by law, to appropriately protect that confidentiality.
- D. Employees shall not transmit confidential county information over the Internet except to the minimum extent necessary to perform their job duties. Confidential information includes, but is not limited to, bank account numbers, credit card numbers, financial information, social security numbers, and any other confidential information pertaining to the County or employee or client of the County.
- E. This policy shall be interpreted and implemented in a manner that complies with HIPAA (Health Insurance Portability and Accountability Act).

### IV. GENERAL GUIDELINES

- A. There should be no expectation of privacy of any materials on the County's systems. The County reserves the absolute right to review and disclose all matters sent over the system or placed into its storage.
- B. Use of the Internet shall be limited to county business purposes. Use of the Internet for non-county business purposes is prohibited. The use of electronic mail for non-county business purposes is prohibited, with the exception of the following: emergency public announcements, emergency school announcements, early-out school notifications, and notifications from schools concerning the illness of a child.
- C. Any use of the County system to obtain or send offensive or sexually explicit material, improperly communicate messages that are derogatory, defamatory or obscene are expressly prohibited at any time.

- D. Employees who download information from the Internet are advised to follow procedures in downloading the information to minimize the risk of contracting a computer virus. Downloading of information shall be limited to county business and subject to review by the Department Head or Information Officer. It is required that every computer system have anti-virus software installed and that every diskette or CD received from a third party be scanned before any employee accesses files on it.
- E. Any violation of the Computer and Internet Policy will subject the employee to discipline up to and including termination.
- F. The employee may be held personally responsible for any criminal or civil action brought about as a result of their activities on the Internet or their failure to comply with these policies regarding computer use and the Internet. Users may be held personally liable for damage to the Cedar County computer system or for damages incurred by Cedar County for damages resulting from the user's failure to comply with these policies.

V. USE OF EQUIPMENT

- A. Any use that violates federal, state, or local law or regulation is expressly prohibited. Specifically but not exclusively the following activities are prohibited:
  - 1. Display or transmission of sexually explicit images, messages, cartoons, or any transmission or use of communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs is prohibited.
  - 2. Knowing or reckless interference with the normal operation of computers, peripherals, or networks is prohibited.
  - 3. Connecting unauthorized equipment to the network for any purpose is prohibited.
  - 4. Running or installing games, files, or other software on Cedar County computers is prohibited, if they are not related to work for Cedar County.
  - 5. Using the County network to gain unauthorized access to any computer system is prohibited.
  - 6. Solicitation is prohibited, whether for charitable, business or personal purposes. Commercial or partisan use is a violation of Iowa law.

VI. NETIQUETTE AND PROTOCOLS

- A. Use of the County's computer systems to access, transmit, store, display or request obscene, pornographic, erotic, profane, racist, sexist or other offensive material (including messages, images, video, or sound) that violates the County's harassment policy or creates an intimidating or hostile work environment is prohibited.

- B. Any use that is deemed to adversely affect the County Government is prohibited.
- C. Use of the County's equipment to transmit any personal opinions about the County or its position on any issue or about any staff member or elected official is strictly prohibited.
- D. There shall be no use of computer equipment or Internet access for personal non-work related purposes, with the exception of the following allowed uses of electronic mail: emergency public announcements, emergency school announcements, early-out school notifications, and notifications from schools concerning the illness of a child.
- E. Users of Computer Systems are further reminded to consider that while they use the County systems, they represent the County just as they would at a county function or in a county vehicle. Visits to web sites and other Internet use may reflect upon the County and should be undertaken in a serious, business like manner.

Any employee who abuses the privilege of county facilitated access to e-mail or the Internet will be subject to corrective action up to and including termination. If necessary, the County also reserves the right to advise appropriate legal officials of any illegal violations.

This policy is subject to change without prior notice.

**Server, Desktop and Wireless Computer System Security Policy  
HIPAA Security Policy #13**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to implement physical safeguards for all Servers and Workstations that access or store electronic PHI, to restrict access to authorized users.

1. Information Technology will ensure that all servers and desktops used to access, transmit, receive or store PHI are appropriately secured.
2. Servers will be located in a physically secure environment.
3. The system administrator or root account will be password protected.
4. A user identification and password authentication mechanism will be implemented to control user access to the server and workstation.
5. A security patch and update procedure will be established and implemented to ensure that all security patches and updates are promptly applied.
6. Servers must be located on a secure network with firewall protection.
7. All unused or unnecessary services shall be disabled.
8. A virus detection system will be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
9. Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:
  - An inactivity timer (screen saver with password protection) or automatic logoff mechanisms must be implemented.
  - The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.
10. Mobile stations that are located or used in open, common, or otherwise insecure areas must also implement the following measures:
  - Secured with the employee, stored in a locked environment or physically secured using a computer anti-theft cable.
  - An inactivity timer (screen saver with password protection) or automatic logoff mechanism must be implemented.
  - Reasonable safeguards used to prohibit unauthorized entities from viewing confidential information such as logins, passwords, or PHI.
11. Personal Digital Assistants (PDAs) and other handheld mobile devices must not be used for long-term storage of PHI. PHI stored on hand held mobile devices must be purged as soon as it is no longer needed on that device.
12. Each mobile system that is used to access, transmit, receive, or store EPHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

PROCEDURE

**Security Patch and Updates**

At least daily, download and install critical patches for the operating system on a PC or Server, or verify that the automatic download is downloading the needed patches.

Any known critical updates for the AS400 should be installed as soon as possible.

**Guidelines on Anti-Virus Prevention**

Recommended processes to prevent virus problems:

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them from your Deleted Items Folder or Trash.
- Delete spam, chain, and other junk email without forwarding or opening.
- Never download files from unknown or suspicious sources.
- Always scan a floppy diskette or CD from an unknown source for viruses before using it.
- Back-up critical data on a regular basis and store the data in a safe place. Backups are performed on the server, NOT ON YOUR INDIVIDUAL PC's.
- On a daily basis, update the anti-virus software definitions/programs.

## Device and Media Control Policy HIPAA Security Policy #14

### POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Electronic equipment and Storage Media used in association with protected health information (PHI) can be a potential source of disclosure when being moved, decommissioned or destroyed. The purpose of this policy is to establish guidelines for the following, the first two are required, the last two addressable;

1. address the final disposition of electronic [PHI], and/or the hardware or electronic media on which it is stored.
2. removal of electronic [PHI] from electronic media before the media is made available for re-use
3. creating a record of the movements of hardware and electronic media and any person responsible therefore
4. creating a retrievable, exact copy of electronic [PHI], when needed, before movement of equipment

### Definitions

Device: Including but not limited to IBM AS400, personal computers, laptops, handheld units, (PDA's).

Storage Media: Including but not limited to disk drives, tapes, floppy disks, CD's, zip disks, flash cards, USB memory sticks, optical disks, and hard copies.

#### 1. Disposal

All PHI on decommissioned devices and storage media must be irretrievably destroyed, in order to protect the confidentiality of the data contained. If the device or media contains PHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data. If the device or media contains the only copy of PHI that is required or needed, a retrievable copy of the PHI must be made prior to disposal.

- a) Removable magnetic "disks" (floppies, ZIP disks, and the like) and magnetic tapes (reels, cartridges) can be "degaussed" by an appropriately-sized and -powered degasser or destroyed.
- b) Fixed internal magnetic storage (such as computer hard drives), as well as removable storage, can be cleansed by a re-writing process. Software is used to over-write all the usable storage locations of a medium. The simplest method is a single over-write; additional security is provided by multiple over-writes with variations of all 0s, all 1s, complements (opposite of recorded character), and/or random characters.
- c) For CD-RW and CD-R only physical destruction will do.
- d) Removable "solid state" storage devices are also now available. These "flash memory" devices are solid state and are non-volatile (the memory maintains data even after all power sources have been disconnected). Examples include CompactFlash, Memory Stick, Secure Digital, SmartMedia and other types of plug-ins, and a range of "mini-" and "micro-drive" flash devices that use USB or FireWire

ports. Secure over-writes (following manufacturer specifications) are possible for these media as well. Neither degaussing nor over-writing offers absolute guarantees.

e) Paper containing sensitive information should be shredded.

2. Media reuse

Any equipment or storage media that contains confidential, critical, internal use only, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.

\*\*See Exhibit A.

3. Record of Movements

When using storage devices and removable media to transport PHI a procedure must be implemented to track and maintain records of the movement of those devices and media and the parties responsible for the device and media during its movement. See Exhibit B.

4. Retrieval of PHI

All original PHI must be backed up on a regular basis. Backup mechanisms must be tested regularly to verify that PHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA's, when storing original PHI.

Backups of original PHI must be stored off-site in a physically secure facility or in a secure location within the facility.

PROCEDURES

**COMPUTER HARDWARE/SOFTWARE/DATA DISPOSAL PROCEDURE**

**Purpose**

Disposal of computer hardware, software and data are an important aspect of computer security. Protected health information should not be released to unauthorized individuals. All County individuals are responsible for taking the appropriate steps, as defined below, to dispose of computer media, to prevent unauthorized release of protected health information.

**Policy**

Delete data on hard drives. Computer hard drives should be erased by the Information Systems Department, or individual authorized by the Information Systems Director. Computer hard drives should be erased using Killdisk software and then they should be destroyed. This software should be obtained from Information Services. Do not make copies of the software. It can be used on one PC at a time. Run the software utilizing the method that makes three passes.

Delete data on floppy disks, CD's, tapes, etc. Submit them to Information Services for disposal. Floppy disks should have a magnet run over them and then they should be taken apart and destroyed. CD's should be physically destroyed. Tapes should have a magnet run over them and then they should be destroyed.

A record should be made of disposals.

## Cedar County Device and Media Disposal

Please Use this form to track all PHI affected Devices and Media to be destroyed. --- MEDIA CONTROLS & DISPOSAL §164.310 USE §164.310 (d) (2) (ii) - ACCOUNTABILITY §164.310 (d) (2) (iii) • Implement Policies for Media Destruction and

Device or Media to be destroyed or re-used.	Department Affected	Date	Type of Media			What actions were taken with the media. Please list what method was used. Was the media reformatted or destroyed	Employee or Business Associate Assigned to this task	Signature of Reviewing/ documenting
			Tape	Diskette, Removable disk, CD, CDRW	Fixed Disk			

**Exhibit B**

Each department head is responsible for maintaining a log of the movement of devices and media containing PHI out of and into the facility. Secure movements within the facility will be the responsibility of the department head. The log below could be used to track these movements.



## **Access Control Policy HIPAA Security Policy #15**

### POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Policy covers procedures for electronic information systems that maintain electronic protected health information (PHI) to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

#### **1. Unique User Identification**

- a. All users that require access to any network, system, or application will be provided with a unique user identification.
- b. Each user's password must meet the following:
  - Passwords must be a minimum of five characters in length.
  - Passwords must incorporate three of the following characteristics:
    1. Any lower case letters (a-z)
    2. Any upper case letters (A-Z)
    3. Any numbers (0-9)
    4. Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # \$ % ^ & \* ( ) \_ - + = { } [ ] : ; " ` | \ / ? < > , . ~ `)
  - Passwords must not be words found in a Dictionary.
  - Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
- c. Users will not share their unique user identification or password with anyone.
- d. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner.
- e. If a user believes their user identification has been compromised, they must report that security incident to Information Services for a new password.
- f. Department Head will insure that passwords are recorded and saved in a secure file that only the Department head or their designee have access too.

#### **2. Emergency Access**

- a. Information Services will establish and implement, as needed, procedures for obtaining necessary electronic PHI during an emergency. Necessary PHI is defined as information if not available could inhibit or negatively affect patient care.
- b. Systems that do not affect patient care are not subject to the emergency access requirement.

#### **3. Automatic Logoff**

- a. Any server or workstation that stores or access PHI will have the password protected screensaver turned on. The system will be configured to lock the server or workstation after 15 minutes or less of inactivity.
- b. When leaving a server or workstation unattended, the users must lock or activate the systems automatic logoff mechanism (e.g. CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing PHI.

#### **4. Encryption and Decryption**

- a. Encryption of PHI as an access control mechanism is not required unless the custodian of said PHI deems the data to be highly critical or sensitive. Encryption of PHI is required in some instances as a transmission control and integrity mechanism.

**5. Firewall Use**

- a. Cedar County's network will implement perimeter security and access control with a firewall.
- b. Firewalls must be configured to support the following minimum requirements:
  - Limit network access to only authorized County users and entities.
  - Limit network access to only legitimate or established connections.
  - Console and other management ports must be secured.
  - Failed access attempts will be logged, if allowed by the system's software.
  - Must be located in a physically secure environment.

**6. Remote Access**

- a. Dialup connections must be approved by the Security Officer and will require written documentation as to why it is needed.
- b. Remote access connections require authentication and encryption mechanisms when connecting via an Internet service provider or dialup connection. Examples include VPN clients and authenticated SSL web sessions.
- c. The following security measures must be implemented for any remote access connection:
  - Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications such as PC Anywhere or GoToMyPC.com are not permitted.
  - Remote access workstations must employ a virus detection and protection mechanism.
- d. All encryption mechanisms implemented will support a minimum of 128-bit encryption.
- e. Any user requesting remote access to the Cedar County network must be approved by the Security Officer and Information Services to ensure that the remote workstation device meets security measures

**7. Wireless Access**

- Wireless access to Cedar County networks is not permitted at this time.

**Audit Controls Policy  
HIPAA Security Policy #16**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Policy covers the hardware, software and/or procedural mechanisms that will be implemented by Cedar County to record and examine activity in information systems that contain or use PHI.

**1. Audit Control Mechanisms**

- a. Information Services will implement system journaling/logging mechanisms for the central AS400 Server regarding PHI.
- b. The system's audit log will include at least User ID, Login Date/Time, and Logout Date/Time.
- c. System audit journals/logs will be reviewed on a regular basis, by the Security Officer.

**EPHI Integrity Policy  
HIPAA Security Policy #17**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to protect electronic PHI from improper alteration or destruction and will implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

**Mechanism to Authenticate Electronic Protected Health Information**

1. Cedar County systems will use mechanisms such as error-correcting memory and RAID disk arrays to protect data from alteration or being destroyed, on the systems that have that capability.
2. Cedar County systems will be protected from data alterations or destruction by viruses or other malicious code.
3. For data integrity during transmission Cedar County will implement a mechanism (FTP or HTTPS) to corroborate that PHI is not altered or destroyed during transmission.

**Person or Entity Authentication Policy  
HIPAA Security Policy #18**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to verify that a person or entity seeking access to electronic PHI is the one claimed.

PROCEDURE

1. All users who use any network, workstation, system, or application that contains PHI will be required to login (provide user authentication) with user id and password.
2. Users must not misrepresent themselves by using another person's User ID and Password.
3. Users are not permitted to allow other persons or entities to use their unique User ID and password.
4. A reasonable effort will be made to verify the identity of the receiving person or entity prior to transmitting PHI.

**Transmission Security Policy  
HIPAA Security Policy #19**

POLICY

Cedar County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Cedar County has adopted this policy to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of and to implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

PROCEDURE

**1. Transmission Security**

- a. All transmissions of PHI files, folders or documents outside the Cedar County network will be secured by using either FTP or HTTPS.
- b. All receiving entities will be authenticated before transmission.
- c. Any transmissions should include only the minimum amount of PHI.
- d. Use of E-mail to transmit PHI can be used if the following conditions are met:
  1. The PHI data must be in a password protected document.
  2. The sender can authenticate the receiver.
  3. The receiver has given permission to have their PHI sent via E-mail.
  4. The receiver has been made aware of the risks involved.
- e. Use of internal E-mail to send PHI is allowed if the following conditions are met:
  1. The PHI data must be in a password protected document.
  2. The minimum amount of PHI is sent.
  3. The E-mail is not forwarded to any parties.

**2. Integrity Controls**

- a. Transmitting PHI via removable media (floppy disk, CDROM, removable hard drive, etc.) will require the documents to be password protected.
- b. All receiving entities will be authenticated before transmission.
- c. Any transmissions should include only the minimum amount of PHI.

**3. Encryption**

- a. All encryptions mechanisms for electronic transmission are to support a minimum of 128-bit encryption.

**Standards Sections Implementation Specifications (R)=Required, (A)=Addressable****Administrative Safeguards** (see § 164.308)

Security Management Process . .164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility ..164.308(a)(2)	(R)
Workforce Security ..... 164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management . 164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training .164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures .....164.308(a)(6)	Response and Reporting (R)
Contingency Plan ..... 164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation ..... 164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.                   164.308(b)(1)	Written Contract or Other Arrangement (R)

**Physical Safeguards** (see § 164.310)

County Access Controls ..... 164.310(a)(1)	Contingency Operations (A) County Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use ..... .. 164.310(b)	(R)
Workstation Security .....164.310(c)	(R)
Device and Media Controls .....164.310(d)(1)	Disposal (R)

Media Re-use (R)  
Accountability (A)  
Data Backup and Storage (A)

**Technical Safeguards** (see § 164.312)

Access Control .....	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls .....	164.312(b)	(R)
Integrity .....	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication .....	164.312(d)	(R)
Transmission Security .....	164.312(e)(1)	Integrity Controls (A) Encryption (A)

This Page Intentionally Left Blank

ORIGINALLY APPROVED AND ADOPTED THE 10<sup>TH</sup> DAY OF APRIL, 2003.  
FIRST REVISION APPROVED THIS 2<sup>ND</sup> DAY OF OCTOBER, 2003.  
SECURITY AMENDMENT APPROVED THIS 18<sup>TH</sup> DAY OF APRIL, 2005

\_\_\_\_\_  
Dennis Boedeker, Chairman of the Board of Supervisors

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Attest: \_\_\_\_\_  
Betty Ellerhoff, Auditor