HIPAA Security Policies and Procedures

Polk County Security Policies and Procedures For the
Health Insurance and Portability Act, of 1996
HIPAA

COUNTIES MUST COMPLY WITH THIS REGULATION BY APRIL 21, 2005.

Effective Date: 4/21/2005

Security Officer: Anthony Jefferson
Polk County
IT

Table of Contents

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 21. 2005.

A small health plan must comply with the applicable requirements no later than April 21, 2006

A health care clearinghouse must comply with the applicable requirements no later than April 21, 2005.

A County that is a covered health care provider must comply with the applicable requirements no later than April 21, 2005.

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 HIPPA 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 an 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 access from obtaining access to electronic PHI.

Implementation Specifications §164.308(3j(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 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 with 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 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 and 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

Purpose

Polk 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 Polk County's approach to compliance with the Security Regulations. Polk County will:

1. Ensure the confidentiality, integrity and availability of all PHI Polk 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 Regulations by its Workforce.

Policy

1) A Hybrid Entity

Polk County is a hybrid entity under HIPAA with both covered and non-covered departments. Polk County hereby designates its HIPAA covered departments as health care components for purposes of the Security Regulations. Polk County's health care components are listed in Exhibit A.

2) Security Personnel and Implementation

Polk County has designated a Security Officer with overall responsibility for the development and implementation of policies for the Security Regulations. The HIPAA Security Officer is Anthony Jefferson in the Information Technology division of General Services. All impacted County departments and offices have acting HIPAA Security Liaisons. The HIPAA Security Liaison is responsible for ensuring that the department:

1. Complies with the HIPAA Security Policies.
2. Maintains the confidentiality of all PHI they are responsible for.

Polk County will implement reasonable and appropriate security measures to comply with security in the Security Regulations. To determine what is reasonable and appropriate, Polk County will take in to account its size, capabilities, technical infrastructure, security capabilities and the costs of the security measures against the potential risks to PHI disclosure.

3) Security Complaints

The Security Officer is responsible for facilitating a process for individuals to file a complaint regarding the handling of PHI by a Polk County Workforce member. The Security Officer is responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

4) Sanctions and Non-Retaliation

Polk County will ensure the appropriate discipline and sanction for employees and any other Workforce members that violate the Security Polices. Polk County will refrain from intimidating or retaliating against any person for exercising his or her rights under the Security Regulations for reporting any concern, issue or practice that such person believes to be in violation of the Security Regulations. Polk County will not require any persons to inappropriately waive any rights to

file a complaint with the Department of Health and Human Services.

5) Security Policies and Procedures

The Polk County HIPAA Security Policies and Security Procedures are designed to ensure compliance with any 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 Polk County's covered entity component parts in accordance with HIPAA Security Policy #9 - Periodic Evaluation of Security Policies and Procedures.

6) Responsibility of All Employees within a HIPAA Covered Department.

Every member of the Polk County Workforce within a HIPAA covered department of Polk County is responsible for being aware of, and complying with, the Security Policies and Security Procedures.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

EXHIBIT A
COMPONENT PARTS

1. Health Care Provider Component Parts
Polk County Health Services
Polk County Health Department
Polk County Attorneys Office
Polk County Sheriff's Office
Polk County Auditor's Office
Polk County Community, Family and Youth Services Department
Polk County General Services

Security Management Policy
HIPAA Security Policy #2

Purpose

Polk 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). Polk 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.

Policy

1. Risk Analysis
   a. Polk County acknowledges the potential vulnerabilities associated with storing PHI and transmitting PHI inside and outside the county.
   b. Polk County will assess such potential vulnerabilities through the following actions:
      • Identify and document all PHI repositories
      • Identify the potential vulnerabilities to each repository
   c. Polk 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. Polk 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. Polk County will implement security measures and safeguards that are reasonable and appropriate for each PHI repository sufficient to reduce risks and vulnerabilities. Polk 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. Polk County will reassess the potential risks and vulnerabilities of PHI repositories as part of an annual review and update the security measures and safeguards.
   c. The security measures and safeguards implemented for each PHI repository will be documented by the Security Officer in conjunction with the HIPAA liaison.

Assigned Security Responsibility Policy

HIPAA Security Policy #3

Purpose

Polk 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.

Policy

Polk County will assign and document the person who is responsible for the development and implementation of the policies and procedures for HIPAA Security. See Exhibit A.

Exhibit A
Designation Security Officer

Security Officer: Anthony Jefferson
Phone: 515-286-3834
E-Mail: Tony.Jefferson@PolkCountyIowa.Gov

Contact Office: Polk County Information Technology
Phone: 515-286-3757 E-Mail:

Workforce Security Policy
HIPAA Security Policy #4

Purpose

Polk 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). Polk 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 Polk County has implemented to ensure that access to PHI is authorized, supervised and appropriate.

Policy

Authorization and/or Supervision of PHI

Polk County has procedures in place to ensure that only users with a need to access PHI are granted access to PHI. Any user needing access to PHI must be approved through their supervisor and department head before being granted access to the PHI.

Workforce Clearance Procedure

Polk County will create procedures to determine that the access to PHI is needed and appropriate for each user. This determination will be made by each department head or supervisor where PHI is involved.

Termination of Access

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

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Security Awareness and Training Policy
HIPAA Security Policy #5

Purpose

Polk 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). Polk 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, procedures for monitoring log-in attempts and reporting discrepancies and procedures for creating, changing and safeguarding passwords.

Policy

1. Security Reminders

a. Polk County has established procedures on how the County departments and offices and users will be-notified of periodic updates of security changes in HIPAA security policies and procedures.

b. Polk County has established procedures on how to notify departments and users of any warnings that are issued for discovered, reported or potential threats.

2. Password Management

a) Information Technology will develop and implement procedures for creating, changing, and safeguarding passwords.

b) These minimum 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.
- A generic user identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to PHI. Access to PHI will be permitted if there is a second unique user ID and password required.
- Elected Official and Department heads will be responsible for making their employees aware of all password–related polices and procedures, and any changes to those policies and procedures.
- Information Technology will be responsible for setting password aging times for systems networks and applications.
- All Polk 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.
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.

Security Training Program

a) Polk 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 Policy
- 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

Violations

Any individual, found to have violated this policy, may be subject to' disciplinary action up to and including termination of employment.

Data Backup and Contingency Planning Policy
HIPAA Security Policy #6

Purpose

Polk 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). Polk 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, of system failure.

Policy

1. Data Backup Plan
    a. Information Technology 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 media used for the backups be stored in a physically secure location off-site.

2. Disaster Recovery Plan
    a. Polk 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. Polk 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. Polk County will assess the relative criticality of specific applications and data in support of other contingency plan components.

Business Associate Contracts and Other Arrangements Policy
HIPAA Security Policy #7

Purpose

Polk 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). Polk 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.

Policy

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 §164.252(e)(1)(ii)(C),when the County is a health that is a government program providing public benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.

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

Access Control Policy
HIPAA Security Policy #8

Purpose

Polk County is committed 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).

Policy

1. Unique User Identification
   a. All users that require access to any network, system, or application will be provided with unique user identification.
   b. Users will not share their unique user identification or password with anyone.
   c. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner
   d. If a user believes their user, identification has been comprised; they must report that security incident to Information Technology for a new password.

2. Emergency Access
   a. Information Technology 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. Firewall Use
   a. Polk 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.
      - Must be located in a physically secure environment.
   c. Information Technology will document the configuration of its firewalls used to protect the networks in Polk County.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

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 Activity Review (R) Information System Activity Review (R)
Assigned Security Responsibility..... §164.308(a)(2)(R)	
Workforce Security 1§64.308(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 ……1§64.308(a)(8)(R)	
Business Associate Contracts and Other Arrangement……. 1§64.308(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)

Contact: Health
515-286 -3759
Revised: 10/04/05 :