Security Policies and Procedures
For the
Health Insurance Portability and Accountability Act
of 1996
HIPAA

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

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.

General Security Compliance Policy

HIPAA Security Policy #1

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to set forth its compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of Protected Health Information ("PHI"). This Policy covers Dickinson County's general approach to compliance with the Security Regulations. As a covered entity under the Security Regulations, Dickinson County must: (1) ensure the confidentiality, integrity and availability of all PHI Dickinson 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; and (4) ensure compliance with the Security Regulations by its Workforce.

Policy

1) A Hybrid Entity
Dickinson County is a hybrid entity with both covered and non-covered functions. Dickinson County hereby designates its HIPAA covered functions as health care components for purposes of the Security Regulations. Dickinson County's health care components are listed in Exhibit A. Exhibit A may be revised from time to time.

2) Security Personnel and Implementation
On behalf of its covered entity component parts, Dickinson County has designated a Security Officer with overall responsibility for the development and implementation of policies that conform to the Security Regulations. The HIPAA Security Officer is Sue Duhn, HIPAA Security Officer, Dickinson County, 1802 Hill Avenue, Spirit Lake, Iowa 51360. The Security Officer has identified a number of departments within the HIPAA covered entity components of Dickinson County. Each department has a HIPAA Security Liaison. The department head of each department will act as the HIPAA Security Liaison. The Security Liaison is responsible for ensuring that the department: (i) complies with the HIPAA Security Policies, (ii) develops and implements department specific HIPAA security procedures for each Security Policy that is applicable to that department, (iii) maintains the confidentiality of all PHI created or received by the department from the date such information is created or received until it is destroyed, and (iv) ensures all Workforce members within the department are trained on the specific policies necessary to comply with the HIPAA Security Regulations. Dickinson County will implement reasonable and appropriate security measures to comply with security in the Security Regulations. To determine what is reasonable and appropriate Dickinson County will take into account its size, capabilities, technical infrastructure, security capabilities, and the costs of the security measures, against the potential risks to PHI exposure.

3) Security Complaints
The Security Officer shall be responsible for facilitating a process for individuals to file a complaint regarding Dickinson County's Security Policies or the handling of PHI by a Dickinson County employee. The Security Officer shall be responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

4) Mitigation, Sanctions and Non-Retaliation
Dickinson County shall mitigate damages for any violation of the Security Regulations and the Dickinson County Security Policies and Procedures. Dickinson County workforce members will refrain from intimidating or retaliating against any person for exercising his or her rights under the Security Regulations or for reporting any concern, issue or practice that such person believes in good faith to be in violation of the Security Regulations or the Dickinson County Security Policies and Procedures. Dickinson

County shall not require any persons to inappropriately waive any rights of such person to file a complaint with the Department of Health and Human Services.

5) Security Policies and Procedures
The Dickinson County HIPAA Security Policies and Procedures are designed to ensure compliance with the Security Regulations. Such Security Policies and Procedures shall be kept current and in compliance with any changes in the law, regulations or practices of Dickinson 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 Dickinson County HIPAA Covered Entity Component Parts
Every member of the Dickinson County Workforce is responsible for being aware of, and complying with, the Security Policies and Procedures.

Violations
Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

EXHIBIT A
COMPONENT PARTS

1. Health Care Provider Component Parts

a) Dickinson County Community Services Office

b) Dickinson County Sheriffôs Department

c) Dickinson County Auditorôs Office

Security Management Policy

HIPAA Security Policy #2

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson 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 the PHI risk analysis that each County Department will conduct, the security measures and safeguards that each County Department will implement for its PHI based upon such risk analysis, and the information systems review activity that each County Department will conduct to ensure the security of such PHI.

Policy

1. **Risk Analysis**
    a. Dickinson County acknowledges the potential vulnerabilities associated with storing PHI and transmitting PHI inside and outside the County.
    b. Dickinson County will assess potential vulnerabilities by:
        - Identify and document all PHI repositories
        - Periodically re-inventory PHI repositories
        - Identify the potential vulnerabilities to each repository
        - Assign a level of risk to each PHI repository
    c. All repositories of PHI will be identified and logged into a database. Each repository will be logged with the appropriate level of file, system, and owner information including, but not limited to:
        - Repository Name (Database, Filing Cabinet)
        - Department Name
        - Department Contact Information
        - Number of Users that access the repository
        - Number of Records
        - System Name
        - System IP Address
        - System Location
        - System Manager
        - System Manager Contact Information
        - Risk Level
    d. Dickinson County will update its PHI inventory at least annually to ensure that the PHI catalogue is up to date and accurate.
    e. Each identified PHI repository will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of its PHI. The following two-dimensional model will be used to assign a risk level to each PHI repository.

        - High Risk ï Repositories with a large number of records accessed by a large numbers of users.

        - Medium Risk ï Repositories with either a large number of records and a small number of users or a small number of records and a large number of users.

        - Low Risk ï Repositories with a small number of records accessed by a small number of users.

f. Dickinson County will reassess the potential risks and vulnerabilities to the integrity, confidentiality, and availability of each PHI repository and the level of risk assigned to each PHI repository at least annually.
g. PHI repositories that otherwise would fall in the low or medium risk categories may be classified as high risk PHI if the sensitivity or criticality of that information makes it appropriate to do so in the reasonable judgment of Dickinson County which is charged with determining the level of risk for each PHI repository.

2. **Risk Management**
   a. Dickinson County must implement security measures and safeguards for each PHI repository sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Dickinson 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. Dickinson County will reassess the potential risks and vulnerabilities of PHI repository as part of a periodic review and update the security measures and safeguards for such PHI repository to reflect any changes in the risks and vulnerabilities assessment.
   c. All Dickinson County networks, systems, and applications are subject to compliance with the Dickinson County Information Security Policy. Networks, systems, and applications that may send, receive, store, or access electronic PHI must also comply with the HIPAA Security Policies, which supercede the Dickinson County Information Security Policy.
   d. The security measures and safeguards implemented for each PHI repository within Dickinson County must be documented and submitted to the HIPAA Security Office or its designee for approval.

3. **Sanctions for Noncompliance**
   a. To ensure that all members of the County Workforce fully comply with the Dickinson County Security Policies, Dickinson County will appropriately discipline and sanction employees and other Workforce members for any violation of the HIPAA Security Policies in accordance with the Dickinson County HIPAA Privacy Policy ï Privacy Compliance which follows the Dickinson County Personnel Policy.

4. **Information System Activity Review**
   a. Internal audit procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
   b. An Audit Control and Review Plan must be created by Dickinson County with the assistance of the IT Department and approved by the HIPAA Security Office. This plan must include:
      - Systems and Applications to be logged
      - Information to be logged for each system
      - Procedures to review all audit logs and activity reports
   c. Security incidents such as activity exceptions and unauthorized access attempts must be detected, logged and reported immediately to the appropriate system management, security and privacy officers in accordance with the HIPAA Security Policy #7 ï Incident Response and Reporting Policy.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Risk Analysis Procedure

HIPAA Risk Analysis

Scope

1. Identifying the scope is probably the most important step in the risk analysis process. The scope provides the analyst with what is covered and what is not covered in the assessment. It identifies what needs to be protected, the sensitivity of what is being protected and to what level and detail. The scope will also identify what systems and applications are included in the assessment.
    a. What needs to be protected?
    b. Who/What are the threats and vulnerabilities?
    c. What are the single points of failure?
    d. What are the implications if they were damaged or lost?
    e. What is the value to the organization?
    f. What can be done to minimize exposure to the loss or damage?

Collecting data

This step involves collecting all policies and procedures currently in place and identifying those that are missing or undocumented. Interviews with key personnel can be conducted using questionnaires or surveys to assist in identifying assets and missing or out-of-date documentation. Information on vulnerabilities and threats against the specific systems and services identified can be gathered from various resources.

The Physical Setup

1. Determine what must be protected (assets)
2. The Computer systems
    a. The computer systems: The computer systems are a locus for risks, as so much information resides on them. Like the computers at many counties, they are not backed up according to best practices. They effectively form the largest single point of potential failure for the County.
    b. Information (on those computer systems and elsewhere) being stolen from the server is a potential nightmare. This threat to the confidentiality, integrity, and availability of information has a huge potential impact.
    c. Miscellaneous equipment
    d. Paper records
    e. The website
    f. Miscellaneous Threats
    g. There are a few threats to all physical assets that do not fall neatly under just one category above. A tornado, for example, could destroy the entire courthouse and its contents in one fell swoop (very high impact to availability of all physical assets).
3. Determine and prioritize the risks. Risk is the chance that a threat will have an impact on your company. In other words, risk is how much you need to worry about a particular threat, as it is the combination of the amount of pain the threat will cause if it happens and how likely the threat is to happen.
4. Assess responses to the risks. A balance must be found between too much security (very restrictive use, high cost) and too little security (unrestricted use, low visible cost, but high danger). It is important that the value of the information and processes in the system is determined, and the risks identified, so that appropriate countermeasures can be implemented. An organization can make three basic responses to a risk, once they have identified and defined it. The first is to accept the risk and work on other things. This is often the best approach for very low risks or ones about which the organization cannot effectively do anything. The second is to try to mitigate the risk. This means trying to reduce the risk by reducing the potential impact, reducing the likelihood that it will affect the organization, or both. For example, you patch your server, thus reducing the likelihood that the new virus for your OS will affect you. The third is to

try to transfer the risk. This means that you get someone else to accept at least some of the risk for you. For example, you buy insurance.

System Risk Analysis Checklist

1. **Computer**
    a. Is the computer backed up regularly?
    b. Is the admin group restricted in membership?
    c. Is an actual login required (disable auto-login)
    d. Are there individual usernames for all employees?
    e. Is display of all passwords/pass phrases restricted?
    f. Is password strength appropriate?
    g. Is a firewall configured?
    h. Is an antivirus program installed and properly configured?
    i. Is the server/switches/hubs/routers connected through a surge protector or UPS and/or power generator?
    j. Are there single points of failure for any services? (internet provider, single directory controller, etc.)
    k. Are there open ports publicly available to network? (conference room, board room, etc.)
    l. Is a password protected screensaver configured?
    m. Is the Guest account disabled?
    n. Is the Administrator account renamed?
    o. Is there a login warning message?
    p. Is the system currently patched to appropriate levels?
    q. Is the system set for Automatic Updates and to ask the user if he/she wishes to install updates?
    r. Is a BIOS password set?

2. **Router**
    a. Has the administrator password been changed?
    b. Is the firmware updated to appropriate levels?
    c. Are ICMP ping requests blocked?
    d. Is Remote Management disabled?
    e. Is Remote Upgrade disabled?
    f. Is IP address filtering enabled and functioning?
    g. Is IP service filtering enabled and functioning?
    h. Is MAC address filtering enabled and working?
    i. Is Virtual Server disabled?
    j. Are unwanted ports shut down to keep them from serving as a starting point of an attack?
    k. Is logging configured and working?
    l. Is the appliance plugged into a surge protector?
    m. Is the firewall set to default Deny all connections from the Internet to the LAN?
    n. Is the router set to obtain a dynamic IP address from the ISP, rather than a static one (if available)?
    o. Has the wireless SSID been changed from ñdefaultò?
    p. Has the wireless channel been changed from the default value?
    q. Is the 128-bit WEP (Wired Equivalent Privacy) protocol enabled?
    r. Is a Virtual Private Network (VPN) Policy in place?
    s. Is the Pre-shared Key strength appropriate?
    t. Is the Encryption Level appropriate?

Policies

1. Analyze the policies and procedures. The review and analysis of the existing policies and procedures is done to gauge the compliance level within the organization. Policies define acceptable use and provide consistency. Policies need to be reviewed periodically to keep them

up to date. They provide a paper trail in cases of due diligence. It is essential that policies be structured in a way that they are as light as possible, without missing any important issues:

a. Simple and practical
b. Easy to manage and maintain
c. Easy to access by people seeking specific information

2. Password policies are necessary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of computer systems. Inadequate password policies can lead to problems.

Analysis of acceptable risks

One of the final tasks is to assess whether or not the existing policies, procedures and protection items in place are adequate. If there are no safeguards in place providing adequate protection, it can be assumed that there are vulnerabilities. A review of the existing and planned safeguards should be performed to determine if the previously known and discovered risks and threats have been mitigated.

Conclusion

In summary the threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of the County. Organizations that do not perform a threat and risk analysis are leaving themselves open to situations that could disrupt, damage or destroy their ability to conduct business. Therefore the importance of performing a threat and risk analysis must be realized by both the staff supporting the infrastructure and those that relies upon it for their business.

Assigned Security Responsibility Policy

HIPAA Security Policy #3

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson 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 for identifying the security official who is responsible for the development and implementation of the policies and procedures for HIPAA Security.

Policy

Dickinson 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.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Exhibit A

Designation of Security Officer

Security Officer: Sue Duhn
Contact Office: Dickinson County Community Services
Address: 1802 Hill Avenue, Spirit Lake, Iowa 51360
Phone: 712-336-0775
E-Mail: sduhn@co.dickinson.ia.us

Workforce Security Policy

HIPAA Security Policy #4

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson 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 Dickinson County has implemented to ensure that Workforce members who work with PHI or in locations where PHI is available are appropriately supervised, that Workforce members are granted appropriate access to PHI, and that Workforce members PHI access is terminated when employment ends or when a determination is made that such access should be terminated or otherwise modified.

Policy

1) Initial Grant of PHI Access and Ongoing Supervision of PHI Access

Dickinson County will create procedures 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 department head before being granted access to PHI. Departments will maintain documentation supporting each users access to all PHI involved. Supervision will be provided for these users so unauthorized access to the PHI is avoided.

2) Assessment of Appropriateness of Access

Dickinson County will create procedures to determine that the access to PHI is needed and appropriate for each user. When PHI is involved the department head will make the determination.

3) Termination of Access to PHI

Dickinson County will develop and implement procedures for terminating access to PHI when the Workforce member's employment ends. This policy will be used in all terminations of employees and when access to PHI is no longer needed. See Exhibit A

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Exhibit A
Termination Check List

1. Department head notifies IT Department and Security Officer.
2. Department head fills out termination checklist.
3. User is either deleted from all systems or user account is made inactive.
    a. User account is made inactive.
        - User is removed from all Active Directory Groups.
        - User is removed from all distribution lists in E-mail.
        - User account password is changed.
        - Voice mail password is changed.
    b. User account is deleted.
        - User home folders are copied to location specified by Department head or designee
4. User profile is removed from all PCs.
5. User is removed from any remote connectivity systems.

IT Employee Termination

1. Administrator passwords changed
    a. All access to server rooms changed.
    b. All documentation returned or accessible to the HIPAA Security Officer.
2. User account made inactive
    a. User is removed from all Active Directory Groups.
    b. User is removed from all distribution lists in E-mail.
    c. User account password is changed.
    d. Voicemail password is changed.
3. User account is deleted.
    a. User home folders are copied to location specified by Department Head or designee.

Information Access Management Policy

HIPAA Security Policy #5

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to ensure that access to PHI is properly authorized. Dickinson County has adopted this policy to ensure that access to PHI is properly authorized. This policy describes how Dickinson County will ensure that access to PHI is assigned and managed.

Policy

1. **Health Care Clearinghouse Functions**
   Dickinson County is not a health care clearinghouse that is a part of a larger organization so Dickinson County has no access by a larger organization.

2. **Access Authorization**

   a. Dickinson County has established procedures for granting access to PHI through a workstation, transaction, program, or process. Procedures will include the following:
      - 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.
      - The IT Department 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 Upon Transfer of Employment within County**
   a. If a Workforce member transfers to another department within the County:

      - The Workforce member's access to PHI within his current Dickinson County Department must be terminated as of the date of transfer. Departments will follow the procedures created for employment termination, including removal of access to County facilities.
      - The Workforce member's new department head is responsible for requesting access to PHI commensurate with the Workforce member's new role and responsibilities.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Security Awareness and Training Policy

HIPAA Security Policy #6

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to provide security awareness and training program for all members of its Workforce. This Policy covers the components of the security awareness and training program. The program will include:

- Åsecurity reminders
- Åprocedures for guarding against, detecting and reporting malicious software
- Åprocedures for monitoring log-in attempts and reporting discrepancies and
- Åprocedures for creating, changing and safeguarding passwords.

Policy

1. **Security Reminders**
    a) Dickinson County must develop and implement procedures to ensure that periodic security updates are issued to the Workforce on changes to Dickinson County's HIPAA Security Policies and/or Dickinson Countyôs Security procedures.
    b) Dickinson County must develop and implement procedures to ensure that warnings are issued to the Workforce of potential, discovered or reported threats, breaches, vulnerabilities or other HIPAA security incidents.
    c) Such procedures must be submitted to and approved by the HIPAA Security Office.

2. **Protection from Malicious Software**
    a) Dickinson County must develop and implement procedures for guarding against, detecting and reporting to the appropriate persons new and potential threats from malicious code such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.
    b) Dickinson County must train its Workforce to identify and protect against malicious code and software.
    c) The IT Department will notify the HIPAA Security Office and its Workforce members 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.
    d) The Dickinson County Workforce will notify the IT Department if a virus, worm or other malicious code has been identified and is a potential threat to other systems or networks.
    e) The IT Department is 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.
    f) 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.

3. **Log-in Monitoring**
    a) The IT Department will implement a mechanism to log and document failed login attempts on each system containing medium and high-risk PHI.
    b) The IT Department will review such log-in activity reports and logs on a periodic basis.
    c) Procedures for reviewing logs and activity reports will be created by the IT Department and detailed in the Audit control review plan.
    d) All failed log-in attempts of a suspicious nature, such as continuous attempts, must be reported immediately to the HIPAA Security Office and Network Administrator.

4. **Password Management**
    a) The IT Department will develop and implement procedures for creating, changing, and safeguarding passwords.
    b) To ensure that passwords created and used by the Dickinson County Workforce to access any network, system, or application used to access, transmit, receive, or store PHI are properly safeguarded and to ensure that the Workforce is made aware of all password related policies, the following minimum procedures must 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 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. An additional unique user identification and password must be supplied to access applications and database systems containing PHI.
        - All passwords will be of sufficient complexity to ensure that is it 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.
        - The IT Department will be responsible for setting password aging times for systems, networks and applications.
        - All Dickinson 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.

5. **Security Training Program**
    a) Dickinson 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 or who set up, manage or maintain systems and workstations that access, receive, transmit, or store PHI are familiar with Dickinson County's HIPAA Security policies and procedures and their responsibilities regarding such policies and procedures. Appropriate training must consist of, but is not limited to, the following requirements:
        - HIPAA Security Policies
        - HIPAA Business Associate Policy
        - HIPAA Sanction Policy
        - Confidentiality, integrity and availability
        - Individual security responsibilities
        - Common security threats and vulnerabilities
    b) 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

c) Dickinson County will maintain documentation of HIPAA training for each of its employees.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Acknowledgement of HIPAA Security Training

I acknowledge that I received training regarding the security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, I acknowledge that I have a general understanding:

1. of the core elements of HIPAA security,
2. of how to contact the County HIPAA Security Officer, and
3. of the County HIPAA Security Policies and Procedures.

_____
Signature of County Employee

_____
Printed Name of County Employee

_____
County Employee Position

_____
Date of Presentation

_____
Signature of Individual Presenting

Incident Response and Reporting Policy

HIPAA Security Policy #7

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to address security incidents. This Policy covers the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes

Policy

1) Common Incident Response and Reporting System

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

2) Reporting and Responding to HIPAA Security Incidents

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

a. Users will notify the IT Department 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 department head.
b. The IT Department will investigate and recommend updates or fixes for security incidents and then notify the Board of Supervisors.
c. The HIPAA Security and Privacy Officer will be notified by the IT Department and will discuss it with the Board of Supervisors.
d. All contact with outside authorities such as local police, FBI, media, etc. will go through the Board of Supervisors.

3) Documentation of Security Incidents

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

4) Mitigation of Harmful Effects of Known Security Incidents

The harmful effects of known security incidents will be mitigated, by following the reporting procedures outlined above for notifying others within Dickinson County of a known incident so that appropriate action may be taken. The HIPAA Security Officer will be notified of viruses and other malicious software and County-wide threats to PHI. Such notifications may be made by way of the County Email distribution list or the HIPAA Security Office. The department head is responsible for propagating these notifications within its County Department and ensuring that appropriate measures are implemented to mitigate the harmful effects of such security threats based on such notifications.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Security Incident Report Form

The purpose of this form is to report the facts pertaining to any known or suspected violation of Dickinson County's security standards or the laws and regulations governing Dickinson County. Although we ask you to provide your name, it is not necessary for you to do so if you wish to make an anonymous report. An anonymous report can be made by completing this form and mailing it to the Security Officer at Dickinson County. If you do not want to give your name, you may call the Security Officer within one week of submitting this report to inquire about the outcome of the investigation.
If you wish to identify yourself in this report, Dickinson County will make every effort to keep your identity confidential, unless you give Dickinson County permission to reveal it. Only the Security Officer, and others designated by the Security Officer, will have access to your report. No disciplinary action or retaliation will be taken against you for making a good faith report of a compliance violation.
Please include all the factual details of the suspected violation, however big or small, to ensure that the Security Officer has all of the information necessary to conduct a thorough investigation.
Please attach additional pages as needed. The information that you provide should include names, dates, times, places and a detailed description of the incident that led you to believe that a violation of Dickinson County's security standards occurred. Please include a copy or a description of any documents that support your concerns.

Date of this report: _____

Name of person making this report (optional): _____

Description of the violation(s): _____

Detailed description of the incident(s) resulting in the violation (include names, dates, times and places):

Name(s) of person(s) involved in the incident and an explanation of their role:

_____

Name(s) of other person(s) having knowledge of the incident: _____

_____

Department where the incident occurred: _____

_____

Date(s) of the incident: _____

Explanation of how you became aware of the suspected violation: _____

_____

Please attach or describe any documents that support your concern (include a description of the documents, the identity of the persons who wrote the documents, the dates of the documents, and the location of the documents).

_____

_____

_____

_____

_____

_____

_____

_____

_____

Form should be mailed to:
HIPAA Security Officer

Security Incident Report Investigation Form

Date of reported concern: _____

Name of person who received the report: _____

Name of person who made the report (state "unknown" if the report was made anonymously):

_____

Date(s) of investigation: _____

Name(s) of person(s) investigating: _____

_____

Name(s) of person(s) interviewed: _____

_____

Description of documents reviewed: _____

_____

_____

Findings: _____

_____

_____

Plan of correction: _____

_____

_____

_____

_____

_____
Signature of Security Officer

Data Backups and Contingency Planning Policy

HIPAA Security Policy #8

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to ensure that its response to an emergency or other occurrence that damages systems that contain PHI complies with the Security Regulations. This Policy covers the procedures for safe guarding data in the event of an emergency, disaster, fire, vandalism, or system failure.

Policy

1. Applications and Data Criticality Analysis

a. Dickinson County will assess the relative criticality of specific applications and data within Dickinson County for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
b. The assessment of data and application criticality should be conducted periodically to ensure that appropriate procedures are in place for data and applications at each level of risk.

2. Data Backup Plan

a. The IT Department 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 must apply to all medium and high-risk files, records, images, voice or video files that may contain PHI.
c. The Data Backup Plan must require that all media used for backing up PHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
d. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard the PHI in an appropriate manner.
e. Data backup procedures outlined in the Data Backup Plan must be tested on a periodic basis to ensure that exact copies of PHI can be retrieved and made available.

3. Disaster Recovery Plan

a. To ensure that Dickinson County can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing PHI, Dickinson County must establish and implement a Disaster Recovery Plan pursuant to which it can restore or recover any loss of PHI and the systems needed to make that PHI available in a timely manner.
b. The Disaster Recovery Plan should include procedures to restore PHI from data backups in the case of a disaster causing data loss.
c. The Disaster Recovery Plan should include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
d. The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.
e. The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that PHI and the systems needed to make PHI available can be restored or recovered.

4. Emergency Mode Operation Plan

a. Dickinson County will establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of PHI while operating in emergency mode.
b. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
c. The Emergency Mode Operation Plan will be documented and easily available to the necessary personnel at all times.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Periodic Evaluation of Security Policies and Procedures Policy

HIPAA Security Policy #9

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to ensure that its Security Policies are up to date and effective in ensuring the confidentiality, integrity and availability of PHI created, received, maintained and transmitted by Dickinson County. This Policy covers the procedures that will ensure that each Security Policy adopted by Dickinson County and each Security Procedure developed and implemented by a County Department is periodically evaluated for technical and non-technical viability.

Policy

1. Periodic Evaluation

a. Dickinson County will evaluate its Security Polices to determine their compliance with the HIPAA Security Regulations. Dickinson County will make the Security Policies compliant with the Security Regulations. Once compliant, Dickinson 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 Officer will review the Policies and Procedures periodically that Dickinson County has adopted for compliance of the Security Regulations.
c. The Security and Privacy Officer will share with the department heads any changes. The department heads will then need to pass any changes onto the employees within that department.
d. Review of the Security Policies and Procedures will be made upon any changes to the HIPAA Security Regulations or Privacy Regulations.
e. Review of the Security Policies and Procedures will be made upon a serious security violation, breach, or other incident.
f. Review of the Security Policies and Procedures will be made upon any change in technology, environmental processes or business processes that may affect HIPAA security.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Security Verification and Validation Procedures

Purpose

Verification and validation procedures are the key elements in assuring Dickinson County that its electronic data is secure. By establishing policies for the protection of your data and information systems, you have established rules by which Dickinson County will operate. The purpose of this policy is to establish guidelines for the enforcement of those rules.

Procedure

The following actions are to be performed by the IT Department. These steps should be performed **every six months**:

1. Physical walk through
   Visually confirm that computers are not accessible to the general public that passwords/pass phrases are not openly displayed in work areas, and that computers are secured when individuals have left the workplace. In addition, check off-site storage for correct backup tape storage.
2. Interview employees
   Verbally survey employees and ask if they have been asked to share their password/pass phrase, if they know about the security policies in place, and if they secure confidential information appropriately.
3. Inspect audit logs
   Determine if system and application logs should be maintained in a form that cannot readily be viewed by unauthorized persons, and backed up on a periodic basis. All logs should be inspected on a periodic basis.
4. Review audit documentation
   Determine if a periodic review of signed confidentiality statements is conducted and if paper logs of who has attended password/pass phrase training is kept.
5. Examine system settings and configuration files
   Inspect workstation, server, router and proxy server configuration files. Check security settings for appropriate access to files.
6. Inspect network environment
   Inspect environment to be sure that temperature and humidity controls are operating in server rooms that UPS batteries are still charged, and that back-up equipment is still functional.
7. Internal intrusion detection
   Execute software inside your network to detect vulnerabilities in existing firewall/network infrastructure. This includes strong password/pass phrase checking.
8. External intrusion detection
   Independent, unbiased third party performs intrusion tests aimed at known vulnerabilities in your company's firewall/network.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Business Associate Contracts and Other Arrangements Policy

HIPAA Security Policy #10

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson 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 §164.502(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 Dickinson 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. Dickinson County will document the satisfactory assurances through a written contract or other arrangement with the business associate.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT (ñAgreementò), entered into and effective this _____ day of _____, 2005, is by and between _____(ñBusiness Associateò) and Dickinson County.

The statements and intentions of the parties, to this Agreement, are as follows:

The U.S. Department of Health and Human Services (ñHHSò), pursuant to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. 160-64) (ñHIPAAò), governs the privacy of individually identifiable health information (ñHIPAA Privacy and Security Provisionsò); obtained, created or maintained by certain entities; and

The HIPAA Privacy and Security Provisions require Dickinson County to enter into this Agreement with Business Associate in order to protect the privacy of individually identifiable health information maintained by Dickinson County (ñProtected Health Informationò or ñPHIò); and

Dickinson County and Business Associate are committed to complying with the HIPAA Privacy and Security Provisions and this Agreement sets forth the terms and conditions pursuant to which PHI that is provided by, or created or received by, Business Associate from or on behalf of Dickinson County, will be handled between Business Associate and Dickinson County and with third parties.

In consideration of the premises and promises contained herein, it is mutually agreed by and between Dickinson County and Business Associate as follows:

SECTION 1
Responsibilities of Business Associate

Section 1.1 Uses and Disclosures of PHI.
Business Associate shall ensure that any director, officer, employee, contractor or other agent of Business Associate does not use or disclose any PHI in any manner that violates either the HIPAA Privacy and Security Provisions or state law. Business Associate may use any PHI it receives from or creates or maintains on behalf of Dickinson County (a) for performance of any contractual obligations between Dickinson County and Business Associate; (b) for performance of its management and administrative functions; (c) for performance of Business Associateôs legal responsibilities, or (d) as other wise required by any federal, state or local law.

Section 1.2 Safeguards of PHI.
Business Associate shall use appropriate administrative, physical and technical safeguards to maintain the security and privacy of PHI and to prevent unauthorized use and/or disclosure of such PHI. In addition, Business Associate shall provide Dickinson County with information concerning the safeguards upon request.

Section 1.3 Disclosures to Third Parties.
Business Associate shall obtain reasonable written assurances from any third party, including subcontractors or agents, to whom PHI will be disclosed. The written statements shall assure (a) that PHI will be held confidentially and used or further disclosed only as required and permitted under either state law or the HIPAA Privacy and Security Provisions; (b) that the third party agrees to be governed by the same restrictions and conditions contained in this Agreement, and (c) that the third party will notify Business Associate of any instances in which confidentiality of PHI has been breached.

Section 1.4 Reporting Unauthorized Uses and Disclosures.
Business Associate shall report to Dickinson County any and all unauthorized uses or disclosures of PHI made by the Business Associate or by any third party of the Business Associate within five (5) days from the date the Business Associate becomes aware of the violation. In addition, Business Associate shall report to Dickinson County any sanction or remedial action taken or proposed to be taken with regard to the unauthorized use or disclosure and will cooperate with Dickinson County in mitigating any harmful effects of such use or disclosure.

Section 1.5 Accounting of Disclosures.
Business Associate shall maintain an accounting of all disclosures of PHI not expressly authorized in this Addendum. The accounting shall include the date of the disclosure, name and address of the individual or entity, which is the recipient of the disclosure, a brief description of the PHI disclosed, and the purpose of the disclosure. Upon written request from Dickinson County, Business Associate shall provide, to Dickinson County, an accounting of all disclosures within ten (10) working days from date of Dickinson County's request.

Section 1.6 Records Available for HHS Inspection.
Business Associate shall make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI received from, created by, or received by Business Associate on behalf of Dickinson County to the Secretary of HHS for purposes of determining Dickinson County's compliance with HIPAA Privacy and Security Provisions.

Section 1.7 Records Available for County Inspection.
Business Associate shall, within ten (10) days of receipt of a written request from Dickinson County, make available, to Dickinson County, all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI for the purpose of enabling Dickinson County to determine Business Associate's compliance with the terms of this Addendum.

Section 1.8 Individual Request for Access.
Within five (5) days from the date Business Associate receives a request by Dickinson County, Business Associate shall permit an individual to access requested PHI that Business Associate maintains. Business Associate shall allow an individual to access, inspect and or copy the requested PHI.

Section 1.9 Amendments to PHI.
Business Associate shall make an amendment to PHI upon request from Dickinson County.

Section 1.10 Records after Termination of Agreement.
Upon termination of the Business Associate and Dickinson County agreement, Business Associate shall return or destroy all PHI that it maintains in any form, and shall retain no copies (of any format) of such information. If Business Associate and Dickinson County agree that the return or destruction of the PHI is not feasible, Business Associate shall continue to extend the protections of this addendum to said PHI, and limit further use of the said PHI to those purposes that make the return or destruction of the PHI infeasible. The provisions of this section shall survive termination or the agreement.

SECTION 2
Responsibilities of Dickinson County

Section 2.1 Authorizations.
Dickinson County shall notify Business Associate of any changes in, or withdrawal of, the consent or authorization provided to Dickinson County by individuals.

Section 2.2 Restrictions.
Dickinson County shall notify Business Associate, in a timely written manner of any restrictions to the use and/or disclosure of PHI agreed to by Dickinson County.

SECTION 3
Term and Termination

Section 3.1 Term.
The initial term of this Agreement shall be for a period of one (1) year, commencing on the date first above written, and shall automatically renew on a year to year basis on the same terms and conditions, unless terminated earlier by either party in accordance with this Agreement.

Section 3.2 Termination.
Dickinson County shall have the right to terminate this Agreement immediately by giving written notice to Business Associate upon the occurrence of Business Associateôs material breach of any of the terms or obligations of this Agreement.

SECTION 4
Notices

Section 4.1 Notices to Dickinson County.
Any notice, request, demand, waiver, consent, approval or other communication to Dickinson County which is required or permitted herein shall be in writing and shall be deemed given only if delivered personally, or sent by registered mail or certified mail, or by express mail courier service, postage prepaid, as follows:

_____ __
_____ __
_____ __
_____ __
Attention: _____

Section 4.2 Notices to Business Associate.
Any notice, request, demand, waiver, consent, approval or other communication to Business Associate which is required or permitted herein shall be in writing and shall be deemed given only if delivered personally, or sent by registered mail or certified mail, or by express mail courier service, postage prepaid, as follows:

_____ __
_____ __
_____ __
Attention: _____

SECTION 5
Other Terms and Conditions

Section 5.1 Amendment.
This Agreement may be amended at any time by the mutual written agreement of the parties. In addition, Dickinson County may amend this Agreement upon sixty (60) days advance notice to Business Associate and if Business Associate does not provide written objection to Dickinson County within the sixty (60) day period, then the amendment shall be effective at the expiration of the sixty (60) day period.

Section 5.2 Regulatory Amendment.
Dickinson County may also amend this Agreement to comply with applicable statutes and regulations and shall give written notice to Business Associate of such amendment and its effective date. Such amendment will not require sixty (60) days advance written notice.

Section 5.3 Entire Agreement.
This Agreement and attachments attached hereto constitute the entire agreement between Dickinson County and Business Associate, and supersedes or replaces any prior agreements between Dickinson County and Business Associate relating to its subject matter.

Section 5.4 Invalidity.
If any term, provision or condition of this Agreement shall be determined invalid by a court of law, such invalidity shall in no way effect the validity of any other term, provision or condition of this Agreement, and the remainder of the Agreement shall survive in full force and effect unless to do so would substantially impair the rights and obligations of the parties to this Agreement.

Section 5.5 No Waiver.
The waiver by either party of a breach or violation of any provisions of this Agreement shall not operate as or be construed to be a waiver of any subsequent breach.

The parties have executed this Agreement hereto, through their duly authorized officials.

COUNTY	**BUSINESS ASSOCIATE**
By: _____	By: _____ __
Print Name: _____	Print Name: _____
Print Title: _____	Print Title: _____
Date: _____	Date: _____

Facility Access Controls Policy

HIPAA Security Policy #11

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to ensure that physical access to PHI is appropriately limited. 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.

Policy

Contingency Operations

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

County Security Plan

Dickinson 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. Dickinson County will create procedures to control and validate employeeôs access to facilities where PHI is available.
2. Dickinson 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. Dickinson County will create procedures to secure the physical locations where PHI data is stored (such as file cabinets).
4. Facilities where PHI is available will provide appropriate access control mechanisms for access to the facility (such as key locks).

Maintenance Records

Dickinson 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.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Workstation Acceptable Use Policy

HIPAA Security Policy #12

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson 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 such functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access PHI.

Policy

1) Compliance with Dickinson County Computer Use Policy
All Dickinson County employees will comply with the Dickinson County Computer Use Policy to ensure that computers that access PHI are used in a secure and legitimate manner. The Dickinson County Computer Use Policy is attached in Exhibit A.

2) Dickinson County Monitoring of Workstation Use
Workforce members that use Dickinson County information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, the Dickinson County IT Department may log, review, or monitor any data (PHI and non-PHI) stored or transmitted on its information system assets.

3) Removal of Workforce Members Privileges
Dickinson County may remove or deactivate any Workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Exhibit A
County Computer Use Policy

Purpose

It is expected that individuals will use the Internet to improve their job knowledge; to access scientific, technical, and other information on topics of relevance to the County; and to communicate with their peers in other government agencies, academia, and industry. Individuals should be aware that when access is accomplished using Internet addresses and e-mail addresses registered to the County, they may be perceived by others to represent the County. Individuals are advised not to use the Internet for any purpose that is not consistent with the mission of the County. The purpose of this policy is to outline electronic information accessibility and usage at the County**,** including the usage of computers, Internet, fax transmittals and electronic mail.

Definitions

Chat Session:	Real time (occurs immediately as opposed to e-mail type communication which has a delay between interaction) discussion over the Internet. When one participant types information, all other participants read it immediately.
Domain Names:	E-mail addresses. (e.g. userx@mybusiness.com)
Individuals:	Full or part-time individuals, emergency, or temporary individuals, individuals of the County; contractors; an intern; or any individual authorized to have access to the County computer hardware or facilities.
File Transfer	The ability to send and receive computer files via the Internet.
Internet	Refers to thousands of interconnected networks, which provide digital pathways to millions of information sites. Users have worldwide access to Internet hosts and their associated applications and databases. Electronic search and retrieval tools permit users to gather information and data from a multitude of sources and to communicate with other users who have related interests.
Internet Activities	Any activity performed over the Internet. For this document's purpose, it would include e-mail, browsing web pages, file transfer, newsgroups and chat sessions.
Internet E-mail:	The process of transmitting electronic mail via the Internet.
Newsgroup:	A discussion about a particular subject consisting of notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups.
Web Page:	A text and/or graphic display of information on the Internet that is created and maintained to represent its sponsor. (e.g. http://www.mybusiness.com)

Policy

County computer systems are for business use and not for personal use. Individuals are permitted to use the Internet while participating in newsgroups, chat sessions, and e-mail discussion groups (list servers), provided these sessions have a direct relationship to the user's job with the County. Individuals should not express personal opinions, even with disclaimer, as any transmission originating from the County could be deemed official.

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.

The following uses of the Internet and/or e-mail using County equipment or facilities are **not** allowed:

1. Retrieving, forwarding, transferring, storing, or printing text and/or graphics which exceeds the bounds of generally accepted standards of good taste and ethics or contain anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability or religious/political beliefs.
2. Engaging in any unlawful activities or any other activities, which would in any way bring discredit to the County.
3. Engaging in personal commercial activities on the Internet, including offering services or merchandise for sale or ordering services or merchandise from on-line vendors.
4. Engaging in any activity that would compromise the security of any government computer. Login passwords/pass phrases are not to be disclosed or shared with anyone.
5. Personally engaging in any fund-raising activity, endorsing any product or services, participating in any lobbying activity, or engaging in any active political activity.
6. Engaging in any activity that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

In order to avoid capacity problems and to reduce the susceptibility of department information technology resources to computer viruses, individuals will comply with the following guidelines:

1. Personal files shall not be obtained via the Internet nor downloaded and stored on individual PC hard drives or on local area network (LAN) file servers.
2. Official video and voice files should not be downloaded from the Internet except when they will be used to serve an approved County function.
3. Individuals will not provide department e-mail addresses to anyone who does not have a legitimate business purpose for sending e-mail messages to the department.

Users are responsible for:

1. Following existing security policies and procedures in their use of Internet services and refraining from any practices that might jeopardize the Countyôs computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.
2. Learning about Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
3. Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act materials, copyrighted materials, and procurement sensitive data.
4. Conducting themselves in a way that reflects positively on the County, since they are identified as the Countyôs individuals on the Internet, as stated above.

Individuals using the County's equipment to access the Internet are subject to having activities monitored by system or security personnel. Use of the County's computers constitutes consent to security monitoring, and individuals should remember that most sessions are not private.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Exhibit B
County Cellular Phone Usage Policy

Principles and Guidelines

1. Respect the rights and sensibilities of others
    b. Cellular phone usage should adhere to the same standards of conduct and confidentiality as any other phone usage as described in the HIPAA Privacy Policies and Procedures Manual.

4. While the County encourages respect for the rights and sensibilities of others, it cannot protect individuals against the existence of unwarranted cellular phone calls.

Implementation

1. All County codes of conduct apply to cellular phone usage as well as to other forms of communication and activity.
2. Department Heads, Elected Officials, or the Board of Supervisors may be empowered to suspend some or all privileges associated with cellular phone usage in cases of misuse or threat to the integrity of all or part of the County.
3. Before any permanent action is taken against an employee, the employer will be advised of the bases for the proposed action and given an opportunity to respond. Concerns about such actions may be raised through the usual administrative channels associated with the County.
4. Where a violation of County policies or applicable law appears to warrant action beyond elimination of cellular phone privileges, the matter may be referred to the Board of Supervisors or to law enforcement authorities.
5. Complaints or concerns about another's use of County cellular phones should be directed to your Department Head.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Server, Desktop and Wireless Computer System Security Policy

HIPAA Security Policy #13

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to set forth the physical safeguards that will apply to hardware that may be used to access, transmit, store or receive PHI. This Policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PHI to ensure that appropriate security is maintained and that access is restricted to authorized users. Each workstation that is used to access, transmit, receive or store PHI must comply with each of the aforementioned measures. If any of the aforementioned measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken:

- The server, desktop computer system, or wireless computer system must be upgraded to support all of the following security measures
- An alternative security measure must be implemented and documented
- The workstation must not be used to send, receive or store PHI.

Policy

1. **Server Security Requirements**
    a. The IT Department will ensure that all servers used to access, transmit, receive or store PHI are appropriately secured in accordance with this Policy.
    b. Servers must be located in a physically secure environment.
    c. The system administrator or root account must be password protected.
    d. A user identification and password authentication mechanism must be implemented to control user access to the system.
    e. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
    f. Servers must be located on a secure network with firewall protection.
    g. All unused or unnecessary services shall be disabled.

2. **Desktop System Security Requirements**
    a. The IT Department will ensure that each desktop system used to access, transmit, receive or store PHI is appropriately secured in accordance with this Policy.
    b. The system administrator or root account must be password protected.
    c. A user identification and password authentication mechanism must be implemented to control user access to the system.
    d. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
    e. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
    f. All unused or unnecessary services must be disabled.
    g. Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:
        - An inactivity timer 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.

3. **Mobile Systems Security Policy**
    a. The IT Department will ensure that all mobile systems used by members to access, transmit, receive or store PHI are appropriately secured in accordance with this Policy.
    b. The system administrator or root account must be password protected.
    c. A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users.
    d. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
    e. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.
    f. All unused or unnecessary services must be disabled.
    g. Mobile stations that are located or used in open, common, or otherwise insecure areas must also implement the following measures:
        - A theft deterrent device such as a laptop locking cable must be utilized when the device is unattended.
        - An inactivity timer or automatic logoff mechanism must be implemented.
        - Reasonable safeguards must be in place prohibit unauthorized entities from viewing confidential information such as logins, passwords, or PHI.
    h. 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, with a storage time not to exceed 30 days.
    i. Each mobile system that is used to access, transmit, receive, or store PHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

System Security Procedure

Purpose

Security of electronic equipment and products is critical to the operation of the County. All persons with access to the equipment and services provided by the County have responsibility to assure protection from misuse and abuse. The purpose of this policy is to establish guidelines for the physical security of all the County's electronic files.

Definitions

Confidential: Information that is considered confidential according to section 22.7 of the Iowa Code. Such information includes (but is not limited to) hospital records, medical records, professional counselor records of the condition, diagnosis, care or treatment of a patient or former patient or a counselee or former counselee, including outpatient and past, present, or future payment for medical treatment. Such information should not be copied or removed from the organizational control without supervisor's authority. Security should be the highest.

Critical: Information that is considered critical to the County's ongoing operations and that could seriously impede them, if made public or shared internally. Such information includes accounting information, business plans, organizational tables, and highly sensitive data. Such information should not be copied or removed from the organizational control without supervisor's authority. Security should be very high.

Internal Use Only: Information not approved for general circulation outside the organization where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility. Examples include: internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.

Portable Devices: Laptops, electronic "Notepads", PDA's, keychain storage devices, security tokens, etc.

Private Documents: Information designated as private, while still work-related. Such information would include: individual evaluations, memos to personnel office, etc. Security at this level is controlled but normal.

Public Documents: Information in the public domain: annual reports, press statements, media presentations, e-mail, etc. which have been approved for public use. Security at this level is minimal.

Procedure

Granting Access

1. All requests for electronic system access must originate from hiring authority.
2. All individuals will sign a confidentiality statement and return it to hiring authority.
3. Upon granting access, the information technology staff will take the following steps:
    a. Assign the data user a unique user identification.
    b. Assign the data user an initial password/pass phrase.
    c. Provide user with a copy of the County Computer Password Policy.
    d. Provide user with adequate password/pass phrase training.

Servers

1. Computer servers will be located in areas where access is limited to authorized persons only. Unauthorized people will not be allowed in these areas without an escort. Areas in which unattended servers are located will be secured with locked doors.
2. The environment for computer equipment will conform to the manufacturers operating specifications for temperature and humidity.
3. Drinking and eating will be prohibited in the immediate vicinity of computer equipment.
4. All servers will be protected from power surges with an appropriate uninterruptible power source. That power source will provide enough capacity to either safely shut-down the equipment or switch to an alternative power source such as a generator in the event of a loss of power.
5. Unauthorized persons with a legitimate need (on behalf of the County), internal or external, will be required to be accompanied by an escort in order to gain access to areas containing confidential or critical information.
6. Servers that are connected to the Internet will be protected by a firewall.
7. A procedure for creating and maintaining backup media, both on-site and off-site must be in place and followed.
8. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons, and backed-up on a periodic basis. All logs must be audited on a periodic basis.
9. Intrusion detection and network monitoring are both on a 24 x 7 basis and all attempted unauthorized access to the network should be logged and reported.

Virus Protection

1. Servers and workstations will be equipped with virus protection software.
2. Virus detection software will be configured to monitor at all times.
3. Virus definitions will be updated on a daily basis.

Workstations

1. Every effort will be made to make sure computer workstations will not be located in areas where unauthorized persons can view healthcare information.
2. If workstations are located in areas where unauthorized persons may be, those workstations must be ñlogged-outò when unattended.

Portable Devices

1. Portable devices are not to be left unattended in high-traffic public areas.
2. Portable devices that contain confidential information must remain on County premises at all times.

Destruction of Storage Media

1. Internal hard drives that contain confidential, critical, internal use only, and/or private information will be erased or removed by the network administrator before the equipment is removed from the premises.
2. External media such as CDôs, floppy disks, backup tapes, etc. will be destroyed before being discarded.

Approved Method of External Access

1. Healthcare information may not be accessed electronically by external parties without the permission of the Information Technology staff. The Information Technology staff must authorize both the method of such access as well as the information that will be accessed.

Device and Media Control Policy

HIPAA Security Policy #14

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. 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 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.

Policy

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) A few kinds of "write-many" optical media (such as CD-RWs) can be processed via an over-write method. This is not the case for the vast majority of "write-once" optical media in use (notably the CD-R). Because such media are optical rather than magnetic, they can not be degaussed. For the write-once variety, 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. Some theorize that with appropriate time and hardware (e.g., an electron microscope), anything can be recovered. Unless, of course, one is willing to disintegrate, incinerate, pulverize, shred, or smelt. As with paper, the method of disposal depends on the perceived risks of discovery, and estimates of the type of threat.

e) Paper containing sensitive information should be shredded. Strip cut shredders (also called straight cut or spaghetti cut) render paper into thin, long strips. Cross-cut shredders (also called confetti cut) provide both length-wise and width-wise dismemberment -- generating from a few to many hundreds of pieces per shredded page.

2. Media reuse

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

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.

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 PDAÕs, when storing original PHI.

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

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Data Backup Procedures

Introduction

Dickinson County backs up the files and data on a regular basis for two reasons:

- To preserve the integrity of the system in the event of a hardware/software failure or physical disaster.
- To provide a measure of protection against human error or the inadvertent deletion of important files.

To provide for these services the files on each server are regularly copied to another storage medium and retained for periods of time. A typical backup solution would copy data to a magnetic tape and that copy would be stored in a separate physical location to avoid destruction of both the original data and the copy in the event of a disaster.

The process adopted by Dickinson County uses those basic principles in a more elaborate fashion. The process in use provides for:

- daily backup of files (M-F)
    - maintained for four weeks
- weekly archive
    - maintained for four weeks

This scheme allows servers to be restored in the event of a disaster with at most one working days of data missing. Individual files can be restored providing they were present on the system during the backup operation, which occurs Monday through Friday evenings.

It is important to have a suitable backup/restore device also stored off-site in the event of a disaster.

Security

Computer security is a primary concern and the backup system is no exception. The specific security mechanisms available depend on the backup product. In any event some precautions and caveats are generally applicable.

- Authorized personnel have access to the data contained in the backup system.
- The backup devices, servers and storage media are in a secure, locked room with limited access.

Backup Schedule

Files are backed up Monday to Friday late at night. Four weeks of backup tapes are maintained and in addition a weekly archive tape is made which is kept for four weeks. The tapes from the previous week backups as well as weekly backups are stored in a separate building to protect against fire/flooding etc.

Requesting a File Restore

In the event you delete a file that is stored on the server and that was on the file server during a scheduled backup then a restore can be requested by phoning the IT help desk and giving the following information:

- Your login name
- The exact name and path of the file that needs restoring(h:\mydir\myfile.doc for example)
- The last date and time that the file was modified (if known).
- Your email address so you can be mailed once the file is restored.
- How long you can wait for the file to be restored. The file will be restored to its location before it was deleted unless otherwise specified.

User Requirements

In order for the backups to work smoothly and be effective there are some responsibilities that each end user has. These are outlined as follows:

- Ensure that you close files that you are working on before leaving work. Otherwise the file may be in an inconsistent state when it is backed up.
- Think twice before deleting files. Restoring files is time consuming and keeps (County) staff from working on other projects.

Failure Notification

If a backup fails for more than one day in a row users will be notified by posting a message. Another message will be posted when the backups have resumed.

Access Control Policy

HIPAA Security Policy #15

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to ensure that access to PHI is only available to those persons or programs that have been appropriately granted such access. 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 under the HIPAA Security Policy #5.

Policy

1) Unique User Identification and Password

a. To uniquely identify and track each user for the purpose of access control to all networks, systems, and applications that contain PHI, and the monitoring of access to the aforementioned networks, systems, and applications, each user must comply with the measures outlined in this Policy.
b. Any users that require access to any network, system, or application will be provided with a unique user identification.
c. Each user's password must meet the following:
    - Passwords must be a minimum of eight 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 (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; ñó| \ / ? < > , . ~`)
    - 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.
d. Users must not allow another user to use their unique user identification or password.
e. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner.
f. Each user must ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications.
g. If a user believes their user identification has been comprised, they must report that security incident to the IT Department for a new password.

2) Emergency Access

a. The IT Department 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 negativity affect patient care.
b. PHI repositories that do not affect an individualõs care are not subject to the foregoing emergency access requirement.

3) Automatic Logoff

a. Servers, workstations, or other computer systems containing PHI repositories will have password protected screensaver turned on. The aforementioned systems must terminate a user session after 15 minutes of inactivity.
b. Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas that access, transmit, receive, or store PHI must employ inactivity timers or automatic logoff mechanisms. (i.e., password protected screensaver that blacks out screen

activity.) The aforementioned systems must terminate a user session after 15 minutes of inactivity.

c. Servers, workstations, or other computer systems that access, transmit, receive, or store PHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
d. When leaving a server, workstation, or other computer system unattended, 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. Dickinson Countyôs 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.
    - Must be located in a physically secure environment.
c. The IT Department will document its configuration of firewalls used to protect the networks in Dickinson County.

6) Remote Access

a. Dialup connections are not allowed at this time.
b. Dialup connections (if allowed), directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.
c. Authentication and encryption mechanisms are required for all remote access sessions to networks via an Internet service provider or dialup connection. Examples of such mechanisms include VPN clients and authenticated SSL web sessions.
d. The following security measures must be implemented for any remote access connection into a secure network containing PHI:
    - 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 systems must employ a mechanism to ñclear outòcache and other session information upon termination of session.
e. Remote access workstations must employ a virus detection and protection mechanism.
f. VPN split-tunneling is not permitted for connections originating from outside the County network.
g. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.
h. The department head to ensure that the remote workstation device being used by said user meets the HIPAA security measures must approve any user requesting remote access to a secure network. The IT Department will ensure that the previous requirement has been satisfied before access is granted.

7) Wireless Access

a. Wireless access to Dickinson County networks is permitted when the following security measures have been implemented:

- Encryption must be enabled.
- MAC-based or User ID/Password authentication must be enabled. MAC based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network.
- All console and other management interfaces have been appropriately secured or disabled.
- Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing PHI-based systems and applications.
- All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Audit Controls Policy

HIPAA Security Policy #16

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. This Policy covers the hardware, software and/or procedural mechanisms that will be implemented by Dickinson County to record and examine activity in information systems that contain or use PHI.

Policy

1. **Audit Control Mechanisms**
    a. The IT Department will implement system logging mechanisms for all systems that contain PHI.
    b. Each system's audit log **must** include, but is not limited to, User ID, Login Date/Time, and Logout Date/Time.
    c. System audit logs must be reviewed on a regular basis.

2. **Audit Control and Review Plan**
    a. An Audit Control and Review Plan must be developed by the IT Department. The plan must include:
        1. systems and applications to be logged
        2. information to be logged for each system
        3. log-in reports for each system
        4. procedures to review all audit logs and activity reports

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

PHI Integrity Policy

HIPAA Security Policy #17

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to outline the procedures to be used to protect PHI from improper alteration and destruction. This policy is to outline the appropriate data authentication measures that Dickinson County must implement to ensure that PHI is not improperly altered or destroyed. Data authentication is the process used to validate data integrity, verify that the data sent is the same data that is received and ensure the integrity of data stored and retrieved.

Policy

Mechanism to Authenticate Electronic Protected Health Information

1. Dickinson County systems will use mechanisms such as error-correcting memory to protect data from alteration or being destroyed.
2. Dickinson County systems will be protected from data alterations or destruction by viruses or other malicious code.
3. For data integrity during transmission Dickinson County will implement a mechanism such as HTTPS to corroborate that PHI is not altered or destroyed during transmission.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Person or Entity Authentication Policy

HIPAA Security Policy #18

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to set forth the authentication requirements for access to Dickinson County PHI. Dickinson County implemented this policy to verify that a person seeking access to electronic PHI is the person claimed.

Policy

1. Dickinson County users seeking access to any network, system, or application that contains PHI will be required to sign in using user id and password.

2. Dickinson County users seeking access to any network, system, or application must not misrepresent themselves by using another personôs User ID and Password.

3. Dickinson County users are not permitted to allow other persons or entities to use their unique User ID and password.

4. A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting PHI.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.

Transmission Security Policy

HIPAA Security Policy #19

Purpose

Dickinson County is committed to conducting business in compliance with all applicable laws, regulations and Dickinson County policies. Dickinson County has adopted this policy to outline the requirements for transmission of Dickinson County PHI to ensure the security and integrity of such PHI. Dickinson County has adopted this policy to guard against unauthorized access to or modification of PHI that is being transmitted over an electronic communications network or via any form of removable media.

Policy

1) Transmission Security

a. All transmissions of PHI files, folders, or documents outside the Dickinson County network will be secured by using HTTPS.
b. Prior to transmitting PHI from the Dickinson County networks to a network outside of the aforementioned networks the receiving person or entity must be authenticated.
c. All transmissions of PHI from the Dickinson County networks to a network outside of the aforementioned networks should include only the minimum amount of PHI.
d. Use of E-mail to transmit PHI can be used only if the following conditions apply:
    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 only if the following conditions apply:
    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.
f. Wireless connections can be used within the Dickinson County network since the connections are secure and encryption is used. Wireless connections outside the Dickinson County network should not be used.

2) Integrity Controls

a. When transmitting PHI via removable media, including but not limited to, floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives, the sending party must:
    1. Use an encryption mechanism to protect against unauthorized access or modification
    2. Authenticate the person or entity requesting said PHI.
    3. Send the minimum amount of said PHI required by the receiving person or entity.
b. If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

3) Encryption

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

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action, as outlined in the Dickinson County Personnel Policy, or pursuant to any collective bargaining agreement/contract for union employees, up to and including termination of employment.