

---

---

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

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

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

**Security Officer:** \_\_\_\_\_

---

---

## Table of Contents

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

---

---

## **Compliance Dates**

### **HIPAA SECURITY**

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

A health plan that is not a small health plan must comply with the applicable requirements no later than April 21, 2005.

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

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

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

---

---

## Documentation Requirements

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

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

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

### **Documentation §164.316(b)(1)**

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

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

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

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

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

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

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

---

---

## General Requirements

### **General Requirements §164.306(a)**

The County will do the following:

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

### **Flexibility §164.306(b)**

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

### **Standards §164.306(c)**

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

### **Implementation Specifications §164.306(d)**

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

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

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

### **Maintenance §164.306(e)**

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

---

---

## Administrative Safeguards

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

---

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

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

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

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

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

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

1. The County will implement:
  - a. **Security Reminders. (Addressable)**  
Periodic security updates.
  - b. **Protection from Malicious Software. (Addressable)**  
Procedures for guarding against, detecting and reporting malicious software.
  - c. **Log-in Monitoring. (Addressable)**  
Procedures for monitoring log-in attempts and reporting discrepancies.
  - d. **Password Management. (Addressable)**  
Procedures for creating, changing and safeguarding passwords.

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

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

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

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

**Contingency Plan §164.308(7)(i)**

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

**Implementation Specifications §164.308(7)(ii)**

1. **Data Backup Plan. (Required)**  
The County will establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.
2. **Disaster Recovery Plan. (Required)**  
The County will establish (and implement as needed) procedures to restore any loss of data.
3. **Emergency Mode Operation Plan. (Required)**  
The County will establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
4. **Testing and Revision Procedures. (Addressable)**  
The County will implement procedures for periodic testing and revision of contingency plans.
5. **Applications and Data Criticality Analysis. (Addressable)**  
The County will assess the relative criticality of specific applications and data in support of other contingency plan components.

**Evaluation (Required) §164.308(8)**

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

---

---

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

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

This standard does not apply with respect to:

- a. The transmission by the County of electronic PHI to a health care provider concerning the treatment of 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.

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

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

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

## **Physical Safeguards**

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

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

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

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

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

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

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

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

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

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

---

---

#### **Workstation Use §164.310(b)**

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

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

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

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

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

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

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

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

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

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

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

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

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

## **Technical Safeguards**

#### **Access Control §164.312(a)(1)**

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

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

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

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

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

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

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

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

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

---

---

**Audit Controls §164.312(b)**

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

**Integrity §164.312(c)(1)**

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

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

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

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

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

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

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

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

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

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

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

---

---

## **General Security Compliance Policy**

### **HIPAA Security Policy #1**

#### **Purpose**

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

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

#### **Policy**

##### **1) A Hybrid Entity**

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

##### **2) Security Personnel and Implementation**

Johnson County has designated a Security Officer with overall responsibility for the development and implementation of policies for the Security Regulations. The HIPAA Security Officers are Jean Schultz and Bill Horning in Information Services. All County departments have named a HIPAA Security Liaison. The HIPAA Security Liaison is responsible for ensuring that the department:

1. Complies with the HIPAA Security Policies.
2. Maintains the confidentiality of all PHI they are responsible for.
3. Trains all Workforce members within the department at the appropriate level of HIPAA training.

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

##### **3) Security Complaints**

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

##### **4) Sanctions and Non-Retaliation**

Johnson County will ensure that appropriate discipline and sanction employees and any other Workforce members for violations of the Security Policies. Johnson County will refrain from intimidating or retaliating against any person for exercising his or her rights under the Security Regulations for reporting any concern, issue or practice that such person believes to be in violation of the Security Regulations. Johnson County will not require any persons to inappropriately waive any rights to file a complaint with the Department of Health and Human Services.

---

---

### **5) Security Policies and Procedures**

The Johnson County HIPAA Security Policies and Security Procedures are designed to ensure compliance with the Security Regulations. Such Security Policies and Security Procedures shall be kept current and in compliance with any changes in the law, regulations or practices of Johnson County's covered entity component parts in accordance with HIPAA Security Policy #9 - Periodic Evaluation of Security Policies and Procedures.

### **6) Responsibility of All Employees within a HIPAA Covered Department**

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

### **Violations**

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

---

---

**EXHIBIT A  
COMPONENT PARTS**

**1. Health Care Provider Component Parts**

Human Services Department

Health Department

Ambulance Department

Sheriff Department

Auditor Department

---

---

## Security Management Policy

### HIPAA Security Policy #2

#### Purpose

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

#### Policy

##### 1. Risk Analysis

- a. Johnson County acknowledges the potential vulnerabilities associated with storing PHI and transmitting PHI inside and outside the County.
- b. Johnson County will assess such potential vulnerabilities by:
  - Identify and document all PHI repositories
  - Periodically re-inventory PHI repositories
  - Identify the potential vulnerabilities to each repository
  - Assign a level of risk to each PHI repository
- c. All repositories of PHI will be identified and logged into a database maintained by Information Services and Department Security Liaisons. The following information will be gathered in this database.
  - 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. Johnson County will update its PHI inventory annually.
- e. Each repository will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of contained PHI.
- f. Each repository will be assign one of the following Risk Level.
  - High Risk – Repositories with a large number of records accessed by a large numbers of users.
  - Medium Risk – 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 – Repositories with a small number of records accessed by a small number of users.
- g. Johnson County will reassess the potential risks and vulnerabilities to the integrity, confidentiality, and availability of each repository and the level of risk assigned to each repository at least annually.

---

---

## 2. Risk Management

- a. Johnson County will implement security measures and safeguards that are reasonable and appropriate for each PHI repository sufficient to reduce risks and vulnerabilities. Johnson 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. Johnson County will reassess the potential risks and vulnerabilities of PHI repositories as part of a periodic review and update the security measures and safeguards.
- c. Johnson County's entire Workforce is subject to compliance with the Johnson County Information Security Policy. Where PHI is involved the HIPAA Security Policies supersede the Johnson County Information Security Policy.
- d. The security measures and safeguards implemented for each PHI repository will be documented by the Network Administrator.

## 3. Sanctions for Noncompliance

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

## 4. Information System Activity Review

- a. Internal audit procedures will be implemented to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports.
- b. An Audit Control and Review Plan will be created and approved by the HIPAA Security Officer. This plan will 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 Information Services in accordance with the HIPAA Security Policy #7 – Incident Response and Reporting Policy.

## Violations

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

---

---

## **Assigned Security Responsibility Policy**

### **HIPAA Security Policy #3**

#### **Purpose**

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

#### **Policy**

Johnson 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 up to and including termination of employment.

---

---

## Exhibit A

<b>Designation of Security Officer</b>
--

Security Officer:

Phone:

E-Mail:

Contact Office:

Phone:

E-Mail:

---

---

<p style="text-align: center;"><b>Workforce Security Policy</b> <b>HIPAA Security Policy #4</b></p>
---

## **Purpose**

Johnson County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Johnson 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 Johnson County has implemented to ensure that access to PHI is authorized, supervised and appropriate. And procedures to terminate access if not necessary.

## **Policy**

### **Authorization and/or Supervision of PHI**

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

### **Workforce Clearance Procedure**

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

### **Termination of Access**

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

## **Violations**

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

---

---

<b>Information Access Management Policy</b>
---

**HIPAA Security Policy #5**

## **Purpose**

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

## **Policy**

### **1. Health Care Clearinghouse Functions**

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

### **2. Access Authorization**

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

### **3. Access Establishment and Modification**

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

## **Violations**

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

---

---

## **Exhibit A**

### **Termination Check List**

1. Department head notifies Information Services
2. Department head or supervisor fills out termination check list.
3. User is either deleted from all system's or user account is made inactive.
  - a. User account is made inactive.
    - User is removed from all distribution lists in E-mail
    - User account 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 PC's.
5. User is removed from any remote connectivity systems.

---

---

## **Security Awareness and Training Policy**

### **HIPAA Security Policy #6**

## **Purpose**

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

## **Policy**

### **1. Security Reminders**

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

### **2. Protection from Malicious Software**

- a) Johnson County will provide training to all its users on how to identify and protect against malicious code and software.
- b) Information Services will develop and implement procedures to detect and guard against malicious code such as viruses, worms, ad ware, and any other computer program or code designed to interfere with normal operation of a system.
- c) A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up to date.
- d) Information Services will notify all departments and users of new and potential threats from malicious code such as viruses, worms, denial of service attacks, and any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.
- e) Departments and users must notify Information Services if a virus, worm or other malicious code has been identified.
- f) Information services will be responsible for ensuring that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.

### **3. Log-in Monitoring**

- a) Information Services will implement a mechanism to log and document failed login attempts on each system containing medium and high-risk PHI.
- b) Information Services 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 Information Services 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 to the HIPAA Security Officer and Network Administrator.

### **4. Password Management**

- 
- 
- a) Information Services will develop and implement procedures for creating, changing, and safeguarding passwords.
- b) These minimum procedures will be followed:
- All County Employees who use a computer or has access to network resources or systems will have a unique user identification and password.
  - All computers, network resources, system and applications will require the user supply a password in conjunction with their unique user identification to gain access.
  - A generic user identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to PHI. Access to PHI will be permitted if there is a second unique user id and password required.
  - All passwords will be of sufficient complexity to ensure that it is not easily guessable.
  - Elected Official and Department heads will be responsible for making their employees aware of all password-related policies and procedures, and any changes to those policies and procedures.
  - Information Services will be responsible for setting password aging times for systems, networks and applications.
  - All Johnson 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) Johnson County will ensuring that its Employees have been given the appropriate level of HIPAA security training so that all Employees who access, receive, transmit or otherwise use PHI are familiar with Security policies and procedures and their responsibilities regarding such policies and procedures. Training will consist of the following:

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

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

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

#### **Violations**

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

---

---

## Incident Response and Reporting Policy

### HIPAA Security Policy #7

#### **Purpose**

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

#### **Policy**

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

Johnson 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 EPHI must be reported and responded to using the following procedures:

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

**3. Documentation of Security Incidents**

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

**4. Mitigation of Known Security Incidents**

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

#### **Violations**

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

---

---

<b>Data Backups and Contingency Planning Policy</b>
---

**HIPAA Security Policy #8**

## **Purpose**

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

## **Policy**

### **1. Data Backup Plan**

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

### **2. Disaster Recovery Plan**

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

### **3. Emergency Mode Operation Plan**

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

### **4. Testing and Revision Procedure**

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

### **5. Applications and Data Criticality Analysis**

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

## **Violations**

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

---

---

<b>Periodic Evaluation of Security Policies and Procedures Policy</b>
---

<b>HIPAA Security Policy #9</b>
---------------------------------

## **Purpose**

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

## **Policy**

### **1. Periodic Evaluation**

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

---

---

<b>Business Associate Contracts and Other Arrangements Policy</b>
---

<b>HIPAA Security Policy #10</b>
----------------------------------

## **Purpose**

Johnson County is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Johnson 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 the Johnson 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. The Johnson 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 up to and including termination of employment.

---

---

## Facility Access Controls Policy

### HIPAA Security Policy #11

#### **Purpose**

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

#### **Policy**

##### **Contingency Operations**

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

##### **County Security Plan**

Johnson 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. Johnson County will create procedures to control and validate employee's access to facilities where PHI is available.
2. Johnson 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. Johnson County will create procedures to secure the physical locations where PHI data is stored; Examples are data centers and file cabinets.
4. Facilities where PHI is available will provide appropriate access control mechanisms for access to the facility; Examples would be key lock, code lock, and badge reader.

##### **Maintenance Records**

Johnson 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 up to and including termination of employment.

---

---

## **Workstation Acceptable Use Policy**

### **HIPAA Security Policy #12**

#### **Purpose**

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

#### **Policy**

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

#### **Violations**

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

---

---

## **Exhibit A County Computer Use Policy**

### **Introduction**

This document provides guidelines for appropriate use of computer facilities and services at Johnson County. Computers, the Internet and electronic mail are powerful research, communication, commerce and time-saving tools that are made available to County employees. The use of this efficient and effective communication tool is critical but, like any tools, computers, the Internet and electronic mail have the potential to be used for inappropriate purposes. Perceptions are important and County employees must constantly be aware of how their actions are perceived by the public.

### **Policy**

The following policies on computer, the Internet and electronic mail usage shall be observed by all Johnson County employees.

Users of the Internet and electronic mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette.

Primary purpose of the Internet and electronic mail is to conduct official business. Occasionally, employees may use the Internet and electronic mail for individual, nonpolitical purposes on their personal time, if such use does not violate the terms and conditions of this policy. Use of the Internet and electronic mail offers employees an opportunity to develop research and communication skills valuable to the effectiveness and efficiency of our County government.

Users should identify themselves properly when using the Internet and electronic mail, conduct themselves professionally, and be aware that their activities reflect on the reputation and integrity of all County employees.

Each user is individually responsible for the content of any communication sent over or placed on the Internet and electronic mail.

All employees have a responsibility to ensure a respectful workplace. County equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons.

Exceptions to this policy are only allowed when pre approved by the department head and deemed necessary for official County business, research or investigatory work.

The following actions are prohibited. It is unacceptable for County Employees to:

Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system.

Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.

View or distribute obscene, pornographic, profane, or sexually oriented material.

Violate laws, rules, and regulations prohibiting sexual harassment.

Engage in any unauthorized activities for personal financial gain.

Place advertisements for commercial enterprises, including but not limited to, goods, services or property.

---

---

Download, disseminate, store or print materials including articles and software, in violation of copyright laws.

Download any software, including but not limited to games, weather bugs, screen savers, toolbars or any other browsing tools without the permission of Information Services.

Violate or infringe on the rights of others.

Conduct business unauthorized by the department.

Restrict or inhibit other users from using the system or the efficiency of the computer systems.

Cause congestion or disruption of networks or systems, including distribution of chain letters.

Transmit incendiary statements, which might incite violence or describe or promote the use of weapons.

Conduct political activity.

Use the system for any illegal purpose.

Disregard for the policies or other improper use of the Internet may result in limited use and/or cancellation of a person's access and/or disciplinary action, up to and including dismissal.

Where a violation of County policies or applicable law appears to warrant action beyond elimination of computer privileges, the matter may be referred to the Board of Supervisors or to law enforcement authorities.

Complaints or concerns about another's use of County computer resources should be directed to your Department Head or Information Services.

Internet and electronic mail may be subject to monitoring.

---

---

<b>Server, Desktop and Wireless Computer System Security Policy</b>
---

**HIPAA Security Policy #13**

## **Purpose**

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

## **Policy**

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

## **Violations**

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

---

---

## Device and Media Control Policy

### HIPAA Security Policy #14

#### Purpose

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

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

#### Definitions

Device: Including but not limited to 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 appropriate 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 PDA's, 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 up to and including termination of employment.

---

---

<b>Access Control Policy</b> <b>HIPAA Security Policy #15</b>
--

## Purpose

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

## Policy

### 1. Unique User Identification

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

### 2. Emergency Access

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

### 3. Automatic Logoff

- a. Any server or workstation that stores or access PHI will have the password protected screensaver turned on. The system will be configured to lock the server or workstation after 15 minutes of inactivity.
- b. Any servers or workstations that are located in locked or secure environments need not implement inactivity timers.
- c. When leaving a server or workstation unattended, the users must lock or activate the systems automatic logoff mechanism (e.g. CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing PHI.

### 4. Encryption and Decryption

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

---

---

## 5. Firewall Use

- a. Johnson County's network will implement perimeter security and access control with a firewall.
- b. Firewalls must be configured to support the following minimum requirements:
  - Limit network access to only authorized County users and entities.
  - Limit network access to only legitimate or established connections.
  - Console and other management ports must be secured.
  - Failed access attempts will be logged.
  - Must be located in a physically secure environment.
- c. Information Services will document the configuration of its firewalls used to protect the networks in Johnson County.

## 6. Remote Access

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

## 7. Wireless Access

- a. Wireless access to Johnson 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.
  - Unmanaged, ad-hoc, or rogue wireless access points are not permitted.
  - All encryption mechanisms implemented will support a minimum of 128-bit encryption.

## Violations

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

---

---

<p style="text-align: center;"><b>Audit Controls Policy</b> <b>HIPAA Security Policy #16</b></p>
--

## **Purpose**

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

## **Policy**

1. **Audit Control Mechanisms**
  - a. Information Services will implement system logging mechanisms for all system that contain PHI.
  - b. Each system's audit log will include at least User ID, Login Date/Time, and Logout Date/Time.
  - c. System audit logs will be reviewed on a regular basis.
  
2. **Audit Control and Review Plan**
  - a. An Audit Control and Review Plan will be developed by Information Services. The plan will 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 up to and including termination of employment.

---

---

<p style="text-align: center;"><b>EPHI Integrity Policy</b> <b>HIPAA Security Policy #17</b></p>
--

## **Purpose**

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

## **Policy**

### **Mechanism to Authenticate Electronic Protected Health Information**

1. Johnson County systems will use mechanisms such as error-correcting memory and RAID disk arrays to protect data from alteration or being destroyed.
2. Johnson County systems will be protected from data alterations or destruction by viruses or other malicious code.
3. For data integrity during transmission Johnson County will implement a mechanism (FTP or 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 up to and including termination of employment.

---

---

<b>Person or Entity Authentication Policy</b>
---

**HIPAA Security Policy #18**

**Purpose**

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

**Policy**

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

**Violations**

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

---

---

<b>Transmission Security Policy</b>
-------------------------------------

<b>HIPAA Security Policy #19</b>
----------------------------------

## **Purpose**

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

## **Policy**

### **1. Transmission Security**

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

### **2. Integrity Controls**

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

### **3. Encryption**

- a. All encryption 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 up to and including termination of employment.

---

---

**Standards Sections Implementation Specifications (R)=Required, (A)=Addressable**

**Administrative Safeguards (see § 164.308)**

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

**Physical Safeguards (see § 164.310)**

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

---

---

**Technical Safeguards** (see § 164.312)

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