Title: Administrative Policy Health Insurance Portability and Accountability Act Security	**Policy No.** Part 5, Staff Policies Chapter 2, Health Information Privacy & Security Section 2
	Effective Date June 20, 2017
Policy Custodian County Manager	**Adoption/Revision Date** June 20, 2017

Adopting Resolution(s): CC17-188

References (Statutes/Resos/Policies): Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. §§ 164.308 to 164.316; Health Information Technology for Economic and Clinical Health Act (HITECH); Information Security Policy; Information Security Advisory Committee Policy; Health Insurance Portability and Accountability Act Policy; Security and Safety Committee; Disposition of County Personal Property Policy, Access Authorization and identification Access Badge Policy; Jefferson County Personnel Rules; Use of Information Technology Resources Policy; ISAC Standards – Information Security Incident Response Guide, Access Management, Account and Password Management for Basic User Accounts, Data Backup and Restoration, Secure Data Deletion, Use of Removable Media; CC05-178, CC07-471

Purpose: To assure that the County's "Health Care Components" (as identified in County Policy Part 5, Chapter 2, Section 1) comply with the security requirements of HIPAA.

Policy: Health Insurance Portability and Accountability Act Security Policy

A. Definitions

1. Covered Employees and Other Individuals: County elected or appointed officials, employees, volunteers, contractors, business partners and vendors that handle or process confidential information or work in areas that handle such information for a County Department/Division or Elected or Appointed Office.

2. Covered Entity: A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

3. Data Breach: A data breach is an Information Security Incident in which sensitive, protected or confidential information is copied, transmitted, viewed, stolen or used by an unauthorized party.

4. Protected Health Information (PHI): PHI is individually identifiable health information that relates to the individual's past, present, or future physical or mental health, provision of health care, or payment for the provision of health care.

5. Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

B. Administrative Safeguards - Security Management (45 C.F.R. § 164.308(a)(1))

1. Risk Analysis (45 C.F.R. § 164.308(a)(1)(ii)(A))
   The Privacy Official and the Security Official (as identified in the Health Insurance Portability and Accountability Act Hybrid and Privacy and Security Officials Designation Policy) shall conduct a risk analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the county at least once every two years. The risk analysis shall:

   a. Include a formal, written assessment of the risks to PHI including the risk of loss, corruption, or misuse of the data.

   b. Identify current measures used to safeguard information and any gaps between current measures and HIPAA security requirements.

   c. Review suspected and known Security Incidents

2. Risk Management (45 C.F.R. § 164.308(a)(1)(ii)(B))

   a. The county has created an Information Security Advisory Committee (ISAC) to prevent the unauthorized loss or exposure of sensitive information, including PHI, that could cause irreparable harm to the county, its employees, and citizens, and that could also subject the county to fines or other sanctions. ISAC committee composition, responsibilities, and procedures are provided for in the Information Security Advisory Committee Policy.

   b. The county has created the Security and Safety Committee to develop and implement security and safety practices to ensure a secure and safe environment within County facilities for clients, employees, and assets. The Security and Safety Committee's composition and responsibilities are provided for in the Security and Safety Committee Policy.

3. Sanctions (45 C.F.R. § 164.308(a)(1)(ii)(C))

   Failure to comply with this Policy may result in loss of privileges and disciplinary action as provided for in the Personnel Rules. Additionally, employees should be aware that the U.S. Department of Health and Human Services' Office for Civil Rights may impose civil money penalties and the U.S. Department of Justice may impose criminal penalties against an individual that fails to comply with HIPAA regulations. The Privacy Official and Security Official, along with Human Resources, shall be responsible for enforcing this Policy.

4. Information System Activity Review (45 C.F.R. § 164.308(a)(1)(ii)(D))

   a. The ISAC shall maintain the ISAC Standard – Information Security Incident Response Guide to capture suspected and known Security Incidents.

   b. The county shall implement a program to review and audit access log-ins and other information system activities. The HIPAA Security and Privacy Officials may conduct routine reviews of information system activities of Covered Employees and Other Individuals if necessary. These reviews must be documented.

c. Suspicious login attempts shall be brought to the attention of the HIPAA Security and Privacy Officials in a timely manner to ensure protection of PHI.

C. Administrative Safeguards - Assigned Security Responsibility (45 C.F.R. § 164.308(a)(2))

1. The Security Officials, as identified in the Health Insurance Portability and Accountability Act Hybrid and Privacy and Security Officials Designation Policy, shall be responsible for the development and implementation of the policies and procedures required under Part 164, Subpart C of HIPAA.

2. The roles and responsibilities to ensure the security of county information in electronic and physical forms is provided for in the Information Security Policy.

3. All members of the workforce have a responsibility to watch for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected privacy and security breaches to their supervisor, or to the Privacy or Security Official. The Privacy Official shall develop a formal reporting process.

D. Administrative Safeguards - Workforce Security (45 C.F.R. § 164.308(a)(3))

1. Authorization and/or Supervision; Workforce Clearance Procedure (45 C.F.R. § 164.308(a)(3)(ii)(A) and (B))

a. The ISAC Standard - Access Management shall be used to ensure only necessary members of the workforce have access to electronic PHI and to prevent access by those workforce members who do not need access to PHI.

b. Appropriate background checks will be conducted on employees who handle PHI. The individuals with security implementation and enforcement authority, as identified in the Health Insurance Portability and Accountability Act Hybrid and Privacy and Security Officials Designation Policy, shall maintain a list of those individuals with access to PHI. The Security Officials shall audit the list at least annually using the ISAC Standard – Access Management.

c. The Access Authorization and Identification Access Badge Policy shall be used to ensure physical access controls in county buildings, facilities, and grounds.

2. Termination procedures (45 C.F.R. § 164.308(a)(3)(ii)(C))

a. The Privacy and Security Officials shall periodically review termination processes to ensure that electronic access is deactivated and that all keys and identification access badges are returned in a timely manner. These reviews shall ensure that employees who remain employed by the County but who no longer require access to electronic PHI, no longer have such access.

b. The individuals with security implementation and enforcement authority, as identified in the Health Insurance Portability and Accountability Act Hybrid and Privacy and Security Officials Designation Policy, shall ensure that identification access badges and office keys are returned and that access to all county computer systems is terminated when a workforce member that worked with PHI is no longer employed by the county.

c. The loss of a key to a work area that contains PHI must be reported to Facilities Management and the Privacy and Security Officials in the Department/Division or Appointed/Elected Official immediately and the locks must be changed.

E. Administrative Safeguards - Information Access Authorization, Establishment, and Modification (45 C.F.R. § 164.308(a)(4)(ii)(B) & (C))

1. County employees with access to PHI shall comply with all requirements of this Policy, the Information Security Policy, the ISAC Standard – Data Encryption, and the ISAC Standard - Access Management.

2. PHI may not be transmitted by email unless the sender is using a secure email system. Employees using email to transmit PHI should actively monitor and manage email mailbox contents. All distribution and email addresses shall be updated to avoid misdirection of information. In the event PHI is misdirected, the employee shall report the inadvertent transmission to their supervisor.

F. Administrative Safeguards - Security Awareness and Training (45 C.F.R. § 164.308(a)(5))

1. The Privacy and Security Officials, and/or individuals with security implementation and enforcement authority shall train employees on HIPAA-related policies and procedures and any substantive amendments as necessary and appropriate for them to carry out their functions. The Privacy and Security Officials and/or individuals with security implementation and enforcement authority shall maintain documentation of the training provided.

2. County staff members with access to PHI shall be periodically made aware of potential security threats and appropriate security measures. The Privacy and Security Officials shall stay abreast of and address security threats.

3. Protection from Malicious Software (45 C.F.R. § 164.308(a)(5)(ii)(B))
The Security Official, in cooperation with the Information Security Advisory Committee, shall develop programs to protect IT resources from malicious software and ensure County systems are regularly updated. Employees shall be trained to report suspected software and shall be tested as needed to ensure employees can identify suspected malicious software.

4. Log-In Monitoring and Password Management (45 C.F.R. § 164.308(a)(5)(ii)(C) & (D))

ISAC Standard –Password Basic User Accounts provides a password management program to ensure that passwords meet security criteria for length and complexity, expire after a certain length of time, and lockout after a certain number of failed attempts.

G. Administrative Safeguards - Security Incident Procedures (45 C.F.R. § 164.308(a)(6))

Response, mitigation, and reporting shall be completed in compliance with the ISAC Standard – Information Security Incident Response Guide. The Information Security Policy assigns the CISO to oversee operation of the ISAC Standard – Information Security Incident Response Guide.

H. Administrative Safeguards - Continuity Plan (45 C.F.R. § 164.308(a)(7))

1. The county shall develop and implement a Business Continuity Plan to respond to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain PHI. The Plan shall contain the following components

    a. Data Back Up and Recovery Plan
    The ISAC Standard - Data Backup and Restoration shall be followed to maintain retrievable exact copies of PHI and restore any loss of data.

    b. PHI Protection
    The county shall ensure the protection and the security of PHI if the county is operating in emergency mode.

    c. Testing and Revision Procedures
    The county shall implement procedures for the periodic testing and revision of the Business Continuity Plan and ISAC Standard - Data Backup and Restoration.

    d. Applications and Data Criticality Analysis
    The county shall assess the relative criticality of specific applications and data in support of other continuity plan components.

I. Administrative Safeguards - Evaluation (45 C.F.R. § 164.308(a)(8))
The county shall perform an evaluation of the county security programs every two years or as needed in response to environmental or operational changes. Changes shall be implemented as needed.

J. Physical Safeguards - Facility Access Controls (45 C.F.R. § 164.310(a)(1))

1. The county shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed pursuant to the Access Authorization and Identification Access Badge Policy.

2. Continuity Operations (45 C.F.R. § 164.310(a)(2)(i))
The county shall establish, and implement as needed, procedures that allow information technology staff access in support of restoration of lost data in the event of an emergency.

3. Facility Security Plan (45 C.F.R. § 164.310(a)(2)(ii))
The county shall safeguard county buildings, facilities, and equipment from unauthorized physical access, tampering, and theft. This includes providing locks on doors to offices that contain equipment used to access PHI.

4. Access Control and Validation Procedures (45 C.F.R. § 164.310(a)(2)(iii))
The county shall control and validate a person’s access to facilities based on their role or function in accordance with the Access Authorization and Identification Access Badge Policy and the ISAC Standard – Access Management. The Divisions, Departments, and Offices that work with PHI shall ensure that only those individuals who must work with PHI as part of their job functions will be given physical access to the equipment used to access PHI.

5. Maintenance Records (45 C.F.R. § 164.310(a)(2)(iv))
   The county shall document security related repairs and modifications, including but not limited to walls, doors, windows, and locks, to areas where PHI is stored. The county shall maintain a record of repairs and ensure that physical safeguards remain in place while repairs or modifications take place.

K. Physical Safeguards –Workstation Use and Security (45 C.F.R. § 164.310(b) and (c))

1. Employees with access to PHI shall ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens. Screen savers or desktops password protections, views of the screen, and other measures may be employed as appropriate to protect PHI. Items must not be left on computer screens where unauthorized disclosure may occur.

2. User accounts shall not be shared with other employees per the ISAC Standard – Account and Password Management for Basic Users.

L. Physical Safeguards - Device and Media Controls (45 C.F.R. § 164.310(d)(1))

1. Receipt and removal of hardware and media that contain PHI into and out of a division/department, and the movement of these items within the division/department shall be managed as detailed in the Disposition of County Personal Property Policy and as follows:

   a. Disposal (45 C.F.R. § 164.310(d)(2)(i))
      Electronic PHI shall be removed from hardware before a device is surplused.

   b. Media Re-Use (45 C.F.R. § 164.310(d)(2)(ii))
      Disks from servers or personal computers that are surplused shall be destroyed or wiped through a secure data wipe program. Magnetic tapes shall be bulk erased before reuse and destroyed rather than being surplused.

   c. Accountability (45 C.F.R. § 164.310(d)(2)(iii))
      The movement of hardware and electronic media that contained PHI, and the person responsible for such movement, shall be documented.

   d. Data Backup and Storage (45 C.F.R. § 164.310(d)(2)(iv))
      Data stored on the county's servers shall be backed up nightly. PHI created or modified on end user devices/media should be transferred to counter servers/storage at the end of each work day for backup.

M. Technical Safeguards - Access Control (45 C.F.R. § 164.312(a)(1))

1. The ISAC Standard - Access Management and Access Authorization and Identification Access Badge Policy shall be used to ensure members of the workforce have only necessary access to PHI and to prevent those workforce members who do not need access to PHI.

2. Unique User Identification (45 C.F.R. § 164.312(a)(2)(i))
   The county shall assign a unique name and/or number for identifying and tracking user identity in accordance with the ISAC Standard – Password Basic User Accounts and ISAC Standard – Access Management.

3. Emergency Access Procedure (45 C.F.R. § 164.312(a)(2)(ii))
   The county shall establish procedures for obtaining necessary PHI during an emergency.

4. Automatic Logoff (45 C.F.R. § 164.312(a)(2)(iii))
   The county shall implement procedures that terminate a session after a determined time of inactivity.

5. Encryption and Decryption (45 C.F.R. § 164.312(a)(2)(iv))
   Employees that transmit PHI through email must use a county secured email service. The email must be encrypted, and the subject line should alert the receiver of the email's security needs.

N. Technical Safeguards - Audit Controls (45 C.F.R. § 164.312(b))

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

O. Technical Safeguards - Integrity (45 C.F.R. § 164.312(c)(1))

   The county shall protect PHI from improper alteration or destruction by implementing a file integrity monitoring system that alerts to any such unauthorized changes.

P. Technical Safeguards - Person or Entity Authentication (45 C.F.R. § 164.312(d))

1. The County shall implement the ISAC Standard - Access Management Standard to ensure that a person seeking access to electronic protected health information is the one claimed.

2. Individuals with security implementation and enforcement authority shall develop additional procedures, standards and other documents to verify the identity of a person requesting disclosure of PHI.

Q. Transmission Security (45 C.F.R. § 164.312(e)(1))

1. Integrity Controls (45 C.F.R. § 164.312(e)(2)(i))
   The County shall implement technical security measures to guard against unauthorized access to and modifications of PHI that is being transmitted over a communications network.

2. Encryption (45 C.F.R. § 164.312(e)(2)(ii))
   The County shall implement encryption of PHI whenever deemed appropriate.

R. Policies and Procedures Documentation Requirements 45 C.F.R. § 164.316(b)(1))

1. All HIPAA policies, procedures, trainings, and other documentation must be maintained for a period of at least six (6) years. All actions, activities, or assessments required by said policies and procedures, including those set out in this Policy, must be documented and maintained for a period of at least six (6) years.

2. Documentation shall be made available as deemed appropriate by the Privacy and Security Officials.

3. All HIPAA policies and procedures shall be reviewed annually. Administrative changes, such as format and document name changes, addition of references to documents created or revised to address regulation requirements, or similar non-material changes may be made without BCC review.