Title: Administrative Policy Health Insurance Portability and Accountability Act Security	**Policy No**. Part 5, Staff Policies Chapter 2, Safety and Health Section 2
	Effective Date October 16, 2007
Policy Custodian Human Resources	**Adoption/Revision Date** October 16, 2007

Adopting Resolution(s): CC07-471

References (Statutes /Resos/Policies): Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. Parts 164.308(a)(1)-164.312(b)(2)(iii); CC05-178

Purpose: To adopt, by Jefferson County, Colorado and its Health Care Benefits Plans, a policy that assures that the components of County and all the health benefits plans that it sponsors or administers comply with the electronic security requirements of the Health Insurance Portability and Accountability Act of 1996, 45 CFR Parts 164.308(a)(1) –164.312(b)(2)(iii) (HIPAA).

Policy: HIPAA Security

A. Definitions

1. Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2. Administrative Safeguards: Administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

3. Authentication: The corroboration that a person is the one claimed.

4. Availability: The property that data or information is accessible and useable upon demand by an authorized person.

5. Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

6. Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

7. Facility: The physical premises and the interior and exterior of a building(s).

8. Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

9. Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

10. Malicious Software: A virus or other software designed to damage or disrupt a system.

11. Password: Confidential authentication information composed of a string of characters.

12. Physical Safeguards: Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

13. Protected Health Information (PHI): PHI is anything that can be used to identify an individual such as private information, facial images, fingerprints, and voiceprints. Also note, health information by itself without the 18 identifiers given below is not considered to be PHI. Example: a dataset of medical insurance plans by themselves do not constitute PHI. However, if the medical insurance plan's dataset includes any of the 18 identifiers, then the entire dataset must be protected since it contains an identifier.

    a. Names;

    b. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:

        (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

        (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

    c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

    d. Phone numbers;

    e. Fax numbers;

    f. Electronic mail addresses;

    g. Social Security numbers;

    h. Medical record numbers;

    i. Health plan beneficiary numbers;

    j. Account numbers;

    k. Certificate/license numbers;

    l. Vehicle identifiers and serial numbers, including license plate numbers;

    m. Device identifiers and serial numbers;

    n. Web Universal Resource Locators (URLs);

    o. Internet Protocol (IP) address numbers;

    p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; and
r. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

14. Security or Security Measures: Encompass all of the administrative, physical, and technical safeguards in an information system.

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

16. Technical Safeguards: The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

17. User: A person or entity with authorized access.

18. Workstation: An electronic, computing device, a laptop or desktop computer, for example or any other device that performs similar functions and electronic media stored in its immediate environment.

B. Administrative Safeguards For HIPAA Final Security Requirements

1. Security Management Process (§164.308(a)(1))
The County shall maintain a formal process by which it assesses risks and takes reasonable steps to protect electronic PHI.

a. Risk Analysis
The County shall assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the County. A formal, written assessment of the risks to electronic PHI including the risk of loss, corruption or misuse of the data shall be prepared as needed. The risk analysis shall identify current measures used to safeguard information and any gaps between current measures and HIPAA security requirements.

b. Risk Management
The County shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The County shall make needed changes and implement new or revised policies and procedures as needed to safeguard electronic PHI.

c. Sanction Policy
The County shall apply appropriate sanctions against employees who fail to comply with the security policies and procedures of the County. The Privacy Officer, Security Official, or designee shall be responsible for enforcing this policy. The Privacy Officer shall maintain records of sanctions taken under this policy for six years from date of the sanction.

d. Information System Activity Review
The County shall track and review security incidents involving files containing electronic PHI. Failed or inappropriate login attempts shall be reviewed at the time they occur.

2. Security Responsibility

   a. The HIPAA Security Official is designated through the HIPPA Policy.

   b. The Security Official is responsible for the development and implementation of this policy.

   c. The Security Official may designate employees to administer portions of this policy as long as the Security Official assures that all designees are adequately trained and responsible with the electronic PHI.

3. Workforce Security (§164.308(a)(3))

   a. Workforce Clearance Procedure
   The Security Official or designee shall determine whether a workforce member's access to electronic PHI is necessary. The County shall ensure members of the workforce have only necessary access to electronic PHI and to prevent those workforce members who do not need access from obtaining access to electronic PHI.

   b. Authorization and/or Supervision
   The County's Security Official or designee shall authorize electronic PHI access to the appropriate employees. The Security Official and all designees shall maintain a list of those individuals with this access. The list shall be updated at least annually.

   c. Termination Procedures
   Department and Division timekeepers shall notify the Security Official and designee, either verbally or in writing, when an authorized workforce member is no longer employed by the County. The Security Official or designee shall notify the Information Technology Services (ITS) Division to terminate access to all County computer systems upon receipt of the notification.

4. Information Access Management (§164.308(a)(4))
   The County shall authorize access to electronic PHI in a manner that is consistent with HIPAA regulations. Access to various types of electronic PHI will be determined by the employee's job functions.

   a. Access Authorization
   County employees with access to electronic PHI may access this information from their personal workstations.

   b. Access Establishment and Modification
   With approval from the Security Official or designee, the ITS Division will establish or modify an employee's right to access a particular workstation, program, transaction or process involving access to electronic PHI. The ITS Division will follow its standard procedure to establish or modify this access.

5. Security Awareness and Training (§164.308(a)(5))
   The County shall train employees on this policy and any substantive amendments as necessary and appropriate for them to carry out their functions. The Privacy Officer and designee appointed by the Security Official shall maintain documentation of the training provided.

   a. Security Reminders
   County staff members with access to electronic PHI shall be periodically made aware of potential security threats and appropriate security measures. The ITS Division designee shall stay abreast of and address security threats.

b. Protection from Malicious Software
The County has the following protections in place: virus scanning software, a firewall, E-mail filters and spam filters.

c. Log-in Monitoring
The County shall have full log-in success monitoring in place for Livelink. For the Novell network, failed log-ins and user location by IP address shall be maintained. Three failed network login attempts shall result in automatic deactivation of the user's access to the network.

d. Password Management
The County shall require passwords for access to Livelink. The password for Livelink shall be the same as the Novell password because authentication is via Novell E-Directory. Password changes shall be required annually.

6. Security Incident Procedures (§164.308(a)(6))

a. Response and Reporting
The ITS Division shall 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. This information will be shared with the Security Official and Privacy Officer. If a workforce member calls the IT help desk and reports that he/she has experienced three failed login attempts, a member of the help desk will reset the individual's password. Repeated failed login attempts will be referred to ITS Security who will address the situation. The Security Official will be made aware of the situation.

7. Contingency Plan (§164.308(a)(7))
The ITS Operations Business Contingency Plan shall be implemented as needed to respond to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI.

a. Data Backup Plan
The County shall create and maintain retrievable exact copies of electronic PHI. Hard copy documents shall be scanned into Livelink by HR; Nightly backups for Livelink shall occur.

b. Disaster Recovery Plan
The ITS Business Continuity Plan shall include procedures to restore any loss of data.

c. Emergency Mode Operation Plan
The County's Emergency Mode Operation Plan shall restore the appropriate files and systems.

d. Testing and Revision Procedure
The County shall continue to test restoration of applications and operating systems to ensure successful restoration of all data access.

e. Applications and Data Criticality Analysis
The County shall assess the relative criticality of specific applications and data in support of other contingency plan components. Details shall be included in the ITS Operations Business Contingency Plan.

8. Evaluation (§164.308(a)(8))
   The County shall perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this policy 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. Changes shall be implemented as needed.

9. Business Associate Contracts and Other Arrangements (§164.308(b)(1))

   a. The 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. The County shall document the satisfactory assurances through a written contract or contract addendum with the business associate.

   b. This standard shall not apply with respect to:

      (1) The transmission by the County of electronic PHI to a health care provider concerning the treatment of an individual.

      (2) 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

      (3) 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.

C. Physical Safeguards For HIPAA Final Security Requirements:

1. Facility Access Controls (§164.310(a)(1))
   The County shall 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.

   a. Contingency Operations
      The County shall establish (and implement as needed) procedures that allow ITS staff access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

   b. Facility Security Plan
      The County shall safeguard equipment from unauthorized physical access, tampering and theft. This includes providing locks on doors to offices that contain equipment used to access electronic PHI.

   c. Access Control and Validation Procedures
      The County shall control and validate a person's access to facilities based on their role or function, including visitor control. The Divisions/Departments that work with electronic PHI shall ensure that only those individuals who must work with electronic PHI as part of their job functions will be given physical access to the equipment used to access electronic PHI.

d. Maintenance Records
The County shall document repairs and modifications to the physical components of a department which are related to security (for example, hardware, walls, doors, and locks). The County shall maintain a record of repairs and modifications that impact the physical security of areas that contain equipment used to access electronic PHI. In addition, the County shall ensure that physical safeguards remain in place while repairs or modifications take place.

2. Workstation Use (§164.310(b))
Employees with access to electronic PHI shall ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens. Screen savers, password protections, views of the screen, and other measures may be employed as appropriate to protect electronic PHI. Items must not be left on computer screens where unauthorized disclosure may occur.

3. Workstation Security (§164.310(c))
Employees with electronic PHI stored on their computer's hard drive shall not share their workstations with employees who have not been granted access to PHI.

4. Device and Media Controls (§164.310(d)(1))
Receipt and removal of hardware and electronic media that contain electronic PHI into and out of a division/department, and the movement of these items within the division/department shall be managed as follows:

a. Disposal
Document destruction schedules shall be built into Livelink. In Livelink, the user requests deletion, which is approved by the Records Manager. The Records Manager performs deletion. as outlined in the Archives and Records Management Policy. Routine deletion is based on an approved records retention schedule.

b. Media Re-Use
Disks from servers or personal computers that are surplused shall be destroyed, not recycled. Magnetic tapes shall be bulk erased before reuse and destroyed rather than being surplused.

c. Accountability
Employees with access to electronic PHI that is stored in places other than the County's servers shall maintain a record of where electronic PHI is stored.

d. Data Backup and Storage
The County will create a retrievable, exact copy of electronic PHI before movement of equipment. Data stored on the County's servers shall be backed up nightly.

D. Technical Safeguards For HIPAA Final Security Requirements:

1. Access Control (§164.312(a)(1))
The County shall allow access to PHI only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Programs are accessed via Novell with strong password authentication. Livelink relies on LDAP using the same UserID and password that is used for Novell. In Livelink, access is specific to the individual.

a. Unique User Identification
The County shall assign a unique name and/or number for identifying and tracking user identity.

b. Emergency Access Procedure
The County shall establish procedures for obtaining necessary electronic PHI during an emergency. In the case of such an emergency, the individual insurance carriers shall be contacted.

c. Automatic Logoff
The County shall implement electronic procedures that terminate an electronic session after a determined time of inactivity. Livelink shall delete the cookie on the workstation when the workstation is rebooted.

d. Encryption and Decryption
Internal e-mail shall be encrypted in GroupWise. E-mail to other agencies shall be encrypted via the TLS standard if the external entity supports it. The County shall provide links to instructions regarding how to implement TLS to other agencies as requested.

2. Audit Controls (§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 electronic PHI. Transaction records in Livelink are tracked via full logging.

3. Integrity (§164.312(c)(1))
The County shall protect electronic PHI from improper alteration or destruction.

4. Mechanism to Authenticate Electronic Protected Health Information (§164.312(c)(2))
The County shall implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner. Automatic control and logging shall be used in Livelink

5. Person or Entity Authentication (§164.312(d))
The County shall implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. In Livelink, authorization shall be granted by the Livelink System Administrators or Livelink EDMS Administrator, depending on the model for which the access is being granted.

6. Transmission Security (§164.312(e)(1))
The County shall implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. Communications from workstations to servers shall be highly constrained by switches.

a. Integrity Controls
The County shall implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of. Livelink shall maintain a complete audit trail and versioning as well.

b. Encryption
The County shall implement a mechanism to encrypt electronic PHI whenever deemed appropriate.