REQUEST FOR BOARD ACTION

HENDERSON COUNTY

BOARD OF COMMISSIONERS

MEETING DATE: **23 March 2005**

SUBJECT: **HIPAA Security Policies**

ATTACHMENT(S):
1. **Proposed Resolution adopting policies**
2. **Proposed policies**

SUMMARY OF REQUEST:

Federal law requires all medical care providers subject to the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, known colloquially as "HIPAA"). In 2002 this Board elected "hybrid entity" status under HIPAA (only those units of Henderson County government which actually fall under HIPAA's reach are required to meet its requirements, rather than all of County government), and in 2003 this Board adopted privacy policies as required by HIPAA. HIPAA now requires adoption of policies addressing electronic data security.

The attached proposed policies, and proposed resolution adopting them, are intended to allow Henderson County government's "Hybrid HIPAA Entity" to meet the security requirements of the Administrative Simplification provisions of HIPAA. They have been drafted by the legal department, and reviewed by appropriate personnel from the information technology, health and emergency medical services departments (the other departments which are a part of the Henderson County "hybrid entity").

COUNTY MANAGER RECOMMENDATION/BOARD ACTION REQUESTED:

County staff will be present and prepared if requested to give further information on this matter. The County manager supports this proposal.

RESOLUTION

WHEREAS, Henderson County government is required to comply with the data security portions of the "Administrative Simplification" provisions of the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, also known as "HIPAA") by 21 April 2005;

WHEREAS, Henderson County government has elected status as a "hybrid entity" under HIPAA regulations;

WHEREAS, Henderson County desires to insure compliance with the Security Rules of the "Administrative Simplification" provisions of HIPAA, and the actions below are necessary in that regard;

NOW, THEREFORE, BE IT RESOLVED by the Board of Commissioners of Henderson County, as follows:

1. Henderson County government hereby adopts the HIPAA Security Policies submitted by the Legal Department of Henderson County. A copy of these policies is filed with the Clerk to the Board of Commissioners, and available for public examination.

2. This resolution shall take effect immediately upon its passage.

ADOPTED this the 23rd day of March, 2005.

HENDERSON COUNTY BOARD OF COMMISSIONERS

BY:_____
WILLIAM MOYER, Chairman

ATTESTED BY:

_____ [OFFICIAL SEAL]
Elizabeth W. Corn, Clerk to the Board

SECURITY POLICIES
PURSUANT TO THE ADMINISTRATIVE SIMPLIFICATION PROVISIONS OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA")

The Board of Commissioners of Henderson County, by resolution adopted 19 June 2002, stated the policy of Henderson County was to timely comply with the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, also known as "HIPAA"). This policy was restated by the Board of Commissioners by resolution dated 19 March 2003. These policies are adopted pursuant to the "Security" provisions of HIPAA.

Henderson County is committed to ensuring the privacy and security of protected health information. Federal, state, and/or local laws and regulations have established standards with which health care organizations must comply to ensure the security and confidentiality of protected health information. To support our commitment to security of patient health information, all employees of Henderson County will receive appropriate training, as required under 45 CFR 164.308.

1. Limitation of Policies

These policies only apply to the departments and units, or portions thereof of Henderson County Government which are a part of the hybrid entity for HIPAA established in the 19 June 2002 resolution of the Board of Commissioners. Such departments and units, or portions there, are referred to herein as "the HIPAA entity".

2. Security Policies

- All workforce members of Henderson County, including management, shall receive training regarding security awareness.
- Computer System Users of Henderson County shall receive training regarding:
    - Protection from malicious software use (including virus protection);
    - Periodic security updates;
    - Log-in; and
    - Password management.
- Henderson County's Data Security Official is responsible for the development and delivery of security training.
- Henderson County's Data Security Official will periodically send out security reminders to make workforce members, as well as agents, and contractors, if necessary, aware of security concerns and initiatives on an ongoing basis.
- Successful completion of periodically recurring training is a prerequisite for system access and a factor of job performance. A secure record will be maintained by the data security official in each department affected by this policy tracking training requirement fulfillment for each individual.]

- Security training policies and procedures may be amended from time to time as necessary to comply with all applicable laws and regulations as well as business associate agreements.

3. **Risk Analysis and Management Standards**

The HIPAA entity shall develop a plan for managing identified risks, prioritizing recovery strategies based on associated risks within available resources, personnel, funding, and tangible assets (computers, space, time). The HIPAA entity shall employ a risk analysis program addressing both intentional and accidental risks.

4. **Risk Management Policy and Procedure**

The HIPAA entity shall implement security measures sufficient to reduce and mitigate risks and vulnerabilities to a reasonable and appropriate level.

The HIPAA entity's security team (designated below) shall receive periodic training/information in security best practices, including issues of labeling of confidential media, avoiding the by-passing of security mechanisms, and the reporting and tracking of security issues.

5. **Sanctions**

The HIPAA entity shall apply appropriate sanctions against workforce members who fail to comply with the security standards, and shall document the evidence that all personnel potentially affected by these sanctions is aware of the sanction process.

6. **Procedures**

Each unit making up the HIPAA entity shall have adopt, employ and enforce procedures for compliance with these policies. These procedures shall include the following:

- Security training will be based on workforce member's job responsibilities, and be applicable to members' daily tasks.
- Include the importance of security responsibility within the workforce member's job description.
- Education and training on security awareness will include, at least, applicable information regarding the following topics:
    - Overall discussion of threats and vulnerabilities specific to electronic protected health information;
    - Information access control;
    - Personnel clearance levels;
    - Incident reporting;
    - Viruses and other forms of malicious software;
    - User log-in;
    - Password maintenance;

- Social engineering;
- HIPAA and organizational privacy and security rules, policies and procedures, and the sanctions, and civil and criminal penalties prescribed for wrongful actions.

- Information access control education will include, at least:
  - Access limitations, including procedures for acquiring additional accesses (or removing accesses) if necessary;
  - Controls in place for regulating access to information.
- Personnel clearance level education will include, at least:
  - Clearance level limitations, including procedures for changing levels if necessary;
  - Controls in place for regulating access to information based on clearance levels.
- Incident reporting education will include, at least:
  - Symptoms of an incident;
  - Persons to notify immediately in the event of a suspected incident;
  - Emphasis on not disclosing the incident to persons without a need to know;
  - Any applicable steps to contain the incident (e.g., disconnect the network cable, but leave the power on).
- Virus protection (malicious code) education will include, at least:
  - Potential harm that can be caused by viruses;
  - Prevention of viruses;
  - What to do if a virus is detected.
- User log-in education will include, at least:
  - Configuration of components to record log-in attempts (both successful and unsuccessful), as well as automated lockout and reporting after [X] failed attempts.
  - Importance of monitoring log-in success of failure.
  - Steps for checking last log-in information, and reporting suspicious information.
  - How to report discrepancies of log-in.
  - User's responsibility to ensure the security of health care information.

- Password management education will include, at least:
    - Rules to be following in creating and changing passwords, including password adequacy (e.g., length, complexity) and frequency considerations; and
    - Importance of keeping passwords confidential, to include storage considerations.
- Social engineering education will include, at least:
    - Emphasis on adhering first to all published policies and procedures, despite claims by persons that they should do otherwise;
    - Emphasis on the practice of verifying an official's identity, position and/or authority prior to taking direction from that person with respect to security measures; and
    - A sampling of common "social engineering" measures and countermeasures.
- Standards, policies and procedures will include, at least:
    - HIPAA security standard overview;
    - Overview of policies and procedures, including how to access and gain clarification regarding such; and
    - Discussion of sanctions and other penalties, as well as the potential for violations to be reported to external agencies.
- Security training will be delivered to all workforce members during initial orientation, and thereafter at least annually.
- Issue periodic reminders and security updates, to include topics on password security, malicious software, incident identification and response, access control, and last log-in monitoring.
- Utilize broadcast e-mail for routine reminders every [Period]. Out of cycle/band reminders can be issued for urgent updates, such as new threats, hazards, vulnerabilities and/or countermeasures.
- The policies and procedures established herein, including all derivative documents regarding security measures will be documented and maintained in a current manner.

7. **Procedural Standards**

- The HIPAA entity shall have one or more internal audit person(s)/team that is/are responsible for review of system activity such as logins, file access, access level modifications, and security incidents.
- The HIPAA entity shall capture all accesses to all protected/confidential information databases on an audit trail log.

8. **Data security official**

- The information technology director of Henderson County shall appoint from among the information technology staff the Henderson County Data Security Official, who is responsible for the development

and implementation of the policies and procedures required. Each department subject to these policies shall designate a departmental data security official to coordinate data security activities in conjunction with the Data Security Official.

- The assignment of responsibility of the Data Security Official shall include the development and implementation of policies and procedures to safeguard electronic protected/confidential information within organizational requirements.

- The assignment of responsibility of the Data Security Official shall include the supervision over the conduct of all personnel in relation to the protection of electronic protected/confidential information.

- The assignment and designation of the Data Security Official shall be documented.