**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: INFORMATION SECURITY STRATEGY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 600** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of information assets by protecting those assets from unauthorized access, modification, destruction, or disclosure.

Hardin County General Hospital will maintain an Information Security Program that complies with core business objectives as well as applicable state and federal regulations. This program as described by Hardin County General Hospital's security policies and supporting plans and procedures, will clearly state the objectives, responsibilities, and enforcement requirements of Hardin County General Hospital.

The purpose of the Hardin County General Hospital Information Security Program is to:

- Establish policies, procedures, plans, and standard tools to secure information in compliance with state and federal security requirements, using minimum levels of industry standards.
- Support Hardin County General Hospital and Hardin County General Hospital's mission to provide continuity of service to customers.
- Maintain unbroken trust with customers and stakeholders through practice of good stewardship of information assets.

This policy applies to all types of sensitive information, including all sensitive information, created by, received, or held by Hardin County General Hospital. This information will be protected in any form including, but not limited to paper, electronic, or oral.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Hardin County General Hospital.

Hardin County General Hospital will implement safeguards determined to be reasonable and appropriate to protect its information assets to maintain the confidentiality, integrity, and availability (CIA) of those assets.

Security policies, plans, and procedures created in support of this Information Security Policy, are organized in five categories (sections) and address at a minimum:

- Administrative safeguards:
  - Security management process
  - Risk analysis
  - Risk management
  - Sanction policy

    - Information system activity review
    - Assigned security responsibility
    - Workforce security
    - Authorization and/or supervision
    - Workforce clearance procedure
    - Termination procedures
    - Information access management
    - Access authorization
    - Access establishment and modification
    - Security awareness and training
    - Security reminders
    - Protection from malicious software
    - Log-in monitoring
    - Password management
    - Security incident procedures
    - Response and reporting
    - Contingency plan
    - Data backup plan
    - Disaster recovery plan
    - Emergency mode operation plan
    - Testing and revision procedures
    - Applications and data criticality analysis
    - Evaluation
    - Business associate agreement and other arrangements
    - Written contract or other arrangement
- Physical safeguards
    - Facility access controls
    - Contingency operations
    - Facility security plan
    - Access control and validation procedures
    - Maintenance records
    - Workstation use
    - Workstation security
    - Disposal
    - Media re-use
    - Accountability
    - Data backup and storage
- Technical safeguards
    - Access control
    - Unique user identification
    - Emergency access procedure
    - Automatic logoff
    - Encryption and decryption
    - Audit controls
    - Integrity
    - Mechanism to authenticate sensitive information
    - Person or entity authentication
    - Transmission security
    - Integrity controls

    - Encryption
- Organizational Framework
    - Policies and Procedures requirement
    - Documentation requirement
- Data Breach
    - Data Breach Management
    - Data Breach Notification
    - Data Breach Notification to HHS
    - Data Breach Notification to Patient
    - Data Breach Notification to Media
- Other Policies
    - Information classification
    - Network security
    - Email security
    - Wireless security

In addition, all security policies, and procedures shall be reviewed and evaluated (based on any environmental and operational changes) on an annual basis by the Compliance Committee or CAH Review Committee.

## II. DEFINITIONS

CIA – Confidentiality, Integrity, and Availability

## III. RESPONSIBILITY

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Compliance with all security policies

The Hardin County General Hospital Compliance Committee is responsible for:

- The development, implementation, and maintenance of Hardin County General Hospital security policies
- Working with employees to develop procedures and plans in support of security policies

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Procedures developed in support of the Information Security Policy will address (but are not limited to):

- Information system activity review
- Workforce clearance
- Termination
- Security incident handling
- Access authorization, establishment, and modification
- Contingency operations procedures
- Physical access control and validation procedures
- Updating maintenance records

- Workstation use
- Media disposal and re-use
- Accountability
- Data backup and storage procedures
- Emergency access
- Automatic logoff

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: SECURITY MANAGEMENT PROCESS POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 601** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement policies and procedures to prevent, detect, contain, and correct security violations.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members.

Hardin County General Hospital will create, administer and oversee policies to ensure the prevention, detection, containment and correction of security violations.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee is responsible for the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets including sensitive information.

The Compliance Committee is responsible for leading compliance activities in the areas of:

- Risk analysis
- Risk management
- Sanction policy
- Information system activity review

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Security management process refers to the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment and correction of security violations.

Hardin County General Hospital will create, administer and oversee policies to ensure the prevention, detection, containment and correction of security violations. Hardin County General Hospital will develop security policies to identify core activities in the areas of risk analysis, risk management, sanctions and information system activity review.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: RISK ANALYSIS POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 602** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.

This policy applies to Hardin County General Hospital in its entirety, including all facilities and systems that process sensitive information.

Hardin County General Hospital will conduct an accurate and thorough assessment of risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information, including EPHI. Such risk analysis activities will be conducted at least once per year and must result in a comprehensive Risk Analysis Report that summarizes the risks, vulnerabilities to the confidentiality, integrity and availability of sensitive information. This report must also identify recommended safeguards and prioritize all such risks and vulnerabilities.

## II. DEFINITIONS

EPHI = Electronic Protected Health Information

## III. RESPONSIBILITY

The Compliance Committee is responsible for coordinating all activities associated with risk analysis. All involved employees who assist with risk analysis activities will be trained in appropriate security compliance requirements and Hardin County General Hospital's security policies with the objective that they understand their responsibilities and duties to reduce the risk of security violations.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.

All risk analysis activities shall be organized into three phases. These phases are:

- Phase I: Documentation Phase
- Phase II: Risk Assessment Phase
- Phase III: Safeguards Determination Phase

The minimal activities that Hardin County General Hospital will conduct in each phase are as follows:

**Phase I: Documentation Phase**

- Identify what sensitive information is collected

- Identify systems with sensitive information
- Document the purpose of these systems
- Document the flow of sensitive information

**Phase II: Risk Assessment Phase**

- Identify vulnerabilities and threats to sensitive information
- Describe the risks
- Identify controls
- Describe the level of risk

**Phase III: Safeguards Determination Phase**

- Recommend safeguards for sensitive information
- Determine residual risk to sensitive information

The results of all identified risk analysis activities along with the safeguard and other recommendations must be summarized with supporting documentation in a Risk Analysis Report.

A Risk Analysis report shall be compiled on a periodic basis and at minimum, annually.

## VI. DOCUMENTATION

Forms related to the risk analysis policy include:

- Risk Assessment Survey
- Risk Analysis Report

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: RISK MANAGEMENT POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 603** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.

This policy applies to Hardin County General Hospital in its entirety, including all facilities and systems that process sensitive information.

Hardin County General Hospital will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee has the responsibility to:

- Ensure that appropriate risk analysis covering, at a minimum, all sensitive information are performed at a frequency of at least once a year
- Approve risk mitigation plans, risk prioritization, and the elimination or minimization of risks
- Facilitate timely actions, decisions and remediation activities

The Compliance Committee must be supported by all system owners, data owners and other managers to identify and prioritize risks to sensitive information. Risk management is an essential management function at Hardin County General Hospital.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce the risk to an acceptable level.

Risk management related activities are essential to help identify critical resources needed to support Hardin County General Hospital and the likely threat to all such resources.

The principal goal of Hardin County General Hospital's risk management policy is to protect the organization, especially its sensitive information, and its ability to perform its mission.

The objective of performing risk management is to enable Hardin County General Hospital to accomplish its mission by:

- Better securing systems that store, process or transmit sensitive information
- Enabling management to make well-informed risk management decisions to justify the expenditures that are a part of the IT and other budgets
- By assisting management in authorizing or evaluating systems on the basis of supporting documentation resulting from the performance of risk management

Risk management consists of three phases:

- Phase I: Risk Assessment
- Phase II: Risk Mitigation
- Phase III: Evaluation and Assessment (Residual Risk)

The activities that Hardin County General Hospital will conduct in each phase are as follows:

**Phase I: Risk Assessment**

- System characterization
- Threat identification
- Vulnerability identification
- Safeguard analysis
- Likelihood determination
- Impact analysis
- Risk Determination
- Safeguard recommendations
- Results documentation

**Phase II: Risk Mitigation**

- Prioritize actions
- Evaluate recommended safeguard options
- Conduct cost-benefit analysis
- Select safeguards
- Assign responsibility
- Develop safeguard implementation plan
- Implement selected safeguards

**Phase III: Evaluation and Assessment (Residual Risk)**

- Evaluate safeguards deployed
- Evaluate security policies

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: SANCTION POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 604** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose of this policy is to apply appropriate sanctions against workforce members who fail to comply with the security policies or procedures of Hardin County General Hospital.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers.

Hardin County General Hospital will ensure all members of its workforce comply with the security policies of the organization as well as state and federal regulations such as HIPAA and the HITECH Act by applying sanction and disciplinary actions appropriate for the breach of policy.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

All individuals identified in the scope of this policy are responsible for:

- Compliance with any sanction that is applied to them under this policy

The Hardin County General Hospital Compliance Committee is responsible for:

- Reviewing reported security incidents and violations of security policy and levying, based on the gravity of the breach, appropriate sanctions upon the workforce member.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will appropriately discipline employees and other workforce members for any violation of security policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings, suspension, and/or immediate dismissal from employment.

In addition, workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.

Hardin County General Hospital will record all disciplinary actions taken in the employment records of the employee.

Hardin County General Hospital will investigate any security incidents or violations and mitigate to the extent possible any negative effects of the incident a timely manner.

Hardin County General Hospital and its workforce members will not intimidate or retaliate against any workforce member or individual that reports the incident.

Hardin County General Hospital will ensure all sanctions in this policy are consistent with HR Policies.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: INFORMATION SYSTEM ACTIVITY REVIEW POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 605** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

This policy applies to Hardin County General Hospital in its entirety, including all systems that process sensitive information.

Hardin County General Hospital will clearly identify all critical systems that process sensitive information. Hardin County General Hospital will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will clearly identify:

- The systems that must be reviewed
- The information on these systems that must be reviewed
- The types of access reports that are to be generated
- The security incident tracking reports that are to be generated to analyze security violations
- The individual(s) responsible for reviewing all logs and reports

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will clearly identify all critical systems that process sensitive information. Hardin County General Hospital will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible, of the following, as reasonable and appropriate:

- User IDs
- Dates and times of log-on and log-off
- Terminal identity, IP address and/or location, if possible
- Records of successful and rejected system access attempts

Hardin County General Hospital will attempt wherever reasonable, appropriate, and technically feasible to record:

- Who (Unique User ID), did
- What action (Read, write, edit, delete, print, etc), to
- What data (Server, DB, instance, table, row, field),
- When (Enterprise wide timestamp), and from
- Where (Terminal ID, IP address, local or remote access)

Safeguards must be deployed to protect against unauthorized changes and operational problems including:

- The logging facility being deactivated
- Alterations to the message types that are recorded
- Log files being edited or deleted
- Log file media becoming exhausted, and either failing to record events or overwriting itself

Procedure(s) related to Information System Activity Review include:

- Security Incident Procedures

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: WORKFORCE SECURITY POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 606** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose of this policy is to implement policies and procedures to ensure that all members of the workforce have appropriate access to sensitive information and to prevent those workforce members who should not have access from obtaining access to sensitive information.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members.

Hardin County General Hospital shall ensure that members of the workforce as well as contractors and others are only accessing those systems and information to which they are authorized.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee is responsible for determining the appropriate classification of information, such as sensitive information and maintains a list that details the type of access for each individual.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Members of the workforce as well as contractors and others shall access only those systems and information to which they are authorized.

Access will be provided on the basis of the Authorization and/or Supervision Policy HITECH 607.

The termination of any member of the workforce will result in the immediate implementation of the activities identified in Termination Procedures.

All members of the workforce will be appropriately trained so they understand Hardin County General Hospital's policies related to accessing authorized information only.

Hardin County General Hospital will continually assess potential risks and vulnerabilities to sensitive information in its possession and develop, implement, and maintain appropriate security measures so that access is only provided to authorized members of the workforce and all such information access is restricted to the minimum necessary to accomplish their job role or function.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: AUTHORIZATION AND/OR SUPERVISION POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 607** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement procedures for the authorization and/or supervision of workforce members who work with sensitive information or in locations where it may be accessed.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members.

Hardin County General Hospital will implement security safeguards to ensure that all members of the workforce who have access to sensitive information, including operations and maintenance employees.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee is responsible for ensuring the implementation of requirements related to the Authorizations and/or Supervision Policy. The activities may include:

- Supervision of some members of the workforce
- Proper access authorizations on the basis of job roles or functions
- Clearance procedures
- Maintenance of access authorization records

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will implement security safeguards to ensure that all members of the workforce who have access to sensitive information, including operations and maintenance employees:

- Need the access they have
- Have the access they need
- Understand the limits of access to sensitive information
- Understand how to authenticate themselves to the system or application

The determination if any access needs to be supervised must be based on the results and recommendations of the Risk Analysis Policy HITECH 602.

Hardin County General Hospital will determine and assign data owners who shall in turn determine what members of the workforce shall have access to what sensitive information.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: TERMINATION PROCEDURE** **Effective Date: 9/1/2012**
**Policy Number: HITECH 608** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement procedures for quickly, securely and completely terminating access to sensitive information when the employment of a workforce member ends.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members including employees, volunteers, temporary workers, contractors, consultants, and any other individuals with access to Hardin County General Hospital systems or facilities.

Hardin County General Hospital will terminate access to all systems and facilities when any member of the workforce has been terminated or no longer requires access to information or facilities in order to perform their assigned job role.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Officer is responsible for ensuring that all activities identified in this Termination Procedure document are followed through and implemented.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

People are the greatest threat to the security of any organization. It is thus important that any termination of a workforce member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments coordinating their activities to ensure:

- Password access is immediately revoked
- Access to all systems and applications is revoked
- The workforce member is removed from any systems or applications that processed sensitive information
- All digital certificates are revoked
- Any tokens or smart cards issued to the workforce member are disabled and returned
- Any keys and IDs provided to the workforce member during their employment are returned
- The workforce member is not provided any access to their desk or office – any such access, if provided, must be limited and carefully supervised

If listed items cannot be returned to Hardin County General Hospital for any reason, compensatory controls must be implemented such as changing locks or remotely disabling tokens.

Termination of access will be verified and segregation of duties will be applied to ensure immediate and complete termination of all access including electronic and physical.

HR must conduct an exit interview and document any issues or concerns related to the workforce member. (See HR Policies for further details).

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: PROTECTION FROM MALICIOUS SOFTWARE POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 609** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement procedures for guarding against, detecting, and reporting malicious software.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Hardin County General Hospital will deploy malicious software identification, prevention, and removal programs or technology at the perimeter (edge) of the network and on all servers including e-mail, and individual end-user systems.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee is responsible for ensuring that malicious software checking programs are installed both on the perimeter (edge) of the network and on individual end-user systems. The Information Technology Department will identify all critical systems and network components that are vulnerable to malicious software. All such identified systems will have malicious software checking capability.

Members of the workforce must not configure or introduce any modifications to systems or applications to prevent the execution of malicious software checking programs. Members of the workforce that suspect any malicious software infection must immediately contact the Information Technology Department or their manager by phone or walk-in – not by e-mail – about the suspected threat.

Members of the workforce must participate in all security awareness training programs and apply the knowledge in preventing, detecting, containing and eradicating malicious software.

## IV. EQUIPMENT

Established system wide antivirus and other removal tools as needed by the Information Technology Department.

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will subscribe to receiving and deploying updates to malicious software checking programs. Hardin County General Hospital will ensure that updates are being received and applied on a daily basis.

Hardin County General Hospital conduct security training that will include information on:

- Potential harm that can be caused by malicious software
- Prevention of malicious software such as viruses
- Steps to take if a malicious software such as a virus is detected

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: SECURITY INCIDENT PROCEDURES** **Effective Date: 9/1/2012**
**Policy Number: HITECH 610** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to thoroughly address security incidents.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. In addition, some third parties such as contractors or vendors, may be required to abide by parts of this policy if required by Hardin County General Hospital in a Business Associate Agreement (BAA).

Hardin County General Hospital will create processes for the identification, reporting, and timely response to real or potential violations of information security or a material breach of any part of Hardin County General Hospital's security policy.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Staying aware of and identifying potential security incidents
- Reporting any suspected security incident to the Compliance Officer
- Assisting the Compliance Officer in ending the security breach and mitigating its harmful effects, if possible

The Compliance Committee is responsible for:

- Maintaining all security incident-related policies and procedures
- Characterizing all reported security incidents as "serious" or "non-serious" as per the guidelines outlined above. The Compliance Committee may take into account their professional expertise and experiences when making these characterizations
- Maintaining procedures for responding to security incidents
- Documenting all reported security incidents and their outcome

The Compliance Committee and other members of management are jointly responsible for:

- Mitigating, to the extent possible, any harmful effects of security incidents
- Deciding when it is appropriate to contact law enforcement officials about a security incident that has been characterized as serious
- The Compliance Officer is responsible for leading compliance activities that bring Hardin County General Hospital into compliance with regulatory requirements.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will maintain procedures for identifying security incidents. A security incident is any breach of security policy, or any activity that could potentially put sensitive information at risk of unauthorized use, disclosure, or modification.

A breach, as defined under the HITECH Act, may have occurred if the incident involved EPHI. A breach is defined as the unauthorized acquisition, access, use, or disclosure of protected information as defined below, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. If a breach has occurred, members of the workforce must immediately follow the instructions in the Data Breach Discovery Policy, HITECH 628.

Incidents will be classified as "serious" or "non-serious." Non-serious incidents generally have the following characteristics:

- It is determined that there was no malicious intent (or the attack was not directed specifically at Hardin County General Hospital associated with the incident and
- It is determined that no sensitive information was used, disclosed, or damaged in an unauthorized manner.

Serious incidents generally have the following characteristics:

- It is determined that there was malicious intent and/or an attack was directed specifically at Hardin County General Hospital.
- It is determined that sensitive information, including EPHI, may have been used, disclosed, or damaged in an unauthorized manner or that this incident may construe a data breach.

All workforce members of Hardin County General Hospital will report any security incident to the Compliance Committee that they become aware of or suspect, as soon as practical. Workforce members will not disclose the incident information to anyone other than the Compliance Officer, Privacy Officer, or Hardin County General Hospital Management Team, and will not disclose any information about the incident to anyone or in any place outside of Hardin County General Hospital.

Hardin County General Hospital will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature.

Incidents characterized as serious by the Compliance Committee will be responded to immediately and reported to all upper-level management.

Hardin County General Hospital will attempt to mitigate any harmful effects, when possible, where a security incident affects customer information.

Procedures related to the Security Incident Response Policy include:

- Security Incident Response Procedure
- Security Incident Documentation Procedure

## VI. DOCUMENTATION

Forms related to the Security Incident Response Procedures include:

- Security Incident Documentation Log

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: RESPONSE AND REPORTING POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 611** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to Hardin County General Hospital; and document security incidents and their outcome.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members, systems, networks, and applications that process, store or transmit sensitive information.

Hardin County General Hospital will identify, research, and respond to any suspected security incident, mitigate, to the extent practicable, any harmful effects of any suspected or actual security incidents, and maintain appropriate documentation for all security incidents.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee is responsible for determining the appropriate level of response to a security incident. All such responses must be in accordance with established policies and procedures. At a minimal, the Compliance Officer and/or his/her team must immediately consider a response that includes:

- Disconnecting the affected system from the network (should not remove power from the system)
- Determining if the incident is accidental or intentional
- Identifying all system-related information such as:
  - Hardware address
  - System name
  - IP address
  - Sensitive data processed by the system
  - Applications installed on the system
  - Location of the system

Members of the workforce will immediately report any and all suspected violations of information security to the Compliance Officer.

All incident reporting and response activities must be conducted strictly on a need-to-know basis.

All members of the workforce will be trained on appropriate reporting of security violations.

The Security Incident Report to be completed by the Compliance Officer or a member of his/her team will include as much information as possible about the following:

- Contact information of the person reporting the incident (name, phone, address, email)

- Date and time of the incident
- Detailed description of the incident
- Any further information, such as unusual activities or individuals associated with the incident

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

If the security incident construes a breach of EPHI, please immediately follow the instructions in the Data Breach Discovery Policy, HITECH 628

This policy requires addressing the following seven steps:

1. Preparing for a Security Incident
2. Detecting and Reporting Security Incidents
3. Assembling the Incident Response Team
4. Limiting Further Damage
5. Gathering Evidence
6. Fixing the Damage
7. Analyzing the Incident

***Step 1: Preparing for a Security Incident***

Every network may at some point be a victim of a computer security incident. System and network administrators must be prepared for security incidents and be able to respond quickly to minimize and repair the damage. Some critical steps that must be addressed are:

- Identify the Security Incident Response Team
- Acquire specialized security training
- Verify the deployment of Intrusion Detection Systems (IDS)
- Verify Data Backup Plan and its implementation

The key is to be prepared so that in the event of a security incident the response is swift and comprehensive in resolving the damage.

***Step 2: Detecting and Reporting Security Incidents***

As soon as a security incident is detected it should be immediately reported to the Compliance Committee or Compliance Officer.

A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. All employees and contractors should be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible. Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

Further, all users of information services should be trained to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their management or to the Compliance Officer as quickly as possible. Users

should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

Procedures will also be established for reporting malfunctions such as those related to software, hardware or any other type.

***Step 3: Assembling the Security Response Team***
The Compliance Committee must meet to evaluate and determine the potential cause of the incident. The following actions should be considered by the team:

- The symptoms of the problem and any messages appearing on the screen should be noted.
- The computer should be isolated, if possible, and use of it should be stopped. The appropriate contact should be alerted immediately. The matter should be reported immediately to the information security manager.

Users should not attempt to remove the suspected software unless authorized to do so.

Appropriately trained and experienced staff authorized by the Compliance Committee should carry out recovery activities.

***Step 4: Limiting Further Damage***
Once the initial data has been collected, immediate steps need to be taken to minimize the spread of the damage. These steps may include disabling Internet access as well as disabling file servers, email servers, communication devices and other systems. The workstation(s) impacted should be isolated, if possible, and their use stopped. If equipment is to be examined, it should be disconnected from any organizational networks before being re-powered. Diskettes and other media should not be transferred to other workstations.

***Step 5: Gathering Evidence***
The Compliance Committee must gather all possible evidence to fully understand the type of attack and its scope. The team needs to address questions such as:

- How many systems are impacted?
- What levels of privileges were accessed?
- How widespread is the vulnerability?
- How far into the internal systems did the intruder get?
- Which systems have been compromised?
- Any risk to sensitive information stored by systems?

All of the information collected should be thoroughly documented and reported. Dedicated systems should be used for incident analysis and forensics. The involved personnel should be trained in the use of such applications.

***Step 6: Fixing the Damage***
Having gathered all the evidence the Compliance Committee must get involved in leading eradication efforts. Malicious files should be deleted, removed or replaced. User accounts and associated passwords may need to be modified or re-created – if there was any evidence of unauthorized access. Data may need to be restored from trusted backups. After the impacted systems are cleaned and protected, they may be brought back online.

Monitor these systems and the infrastructure for other similar, subsequent incidents.

***Step 7: Analyzing the Incident***

The Compliance Committee re-groups to do a post-event de-briefing. The objective is to assess the incident, the response, and identify any specific areas of concern. The team must have a full and complete understanding of the incident and how to prevent such incidents from occurring in the future.

There should also be a review of mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process.

Finally, there should be a formal disciplinary process for employees who have violated organizational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: CONTINGENCY PLAN POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 612** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to 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 sensitive information.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Hardin County General Hospital will develop, maintain, and test a contingency plan. The plan shall be routinely updated plan and include activities for responding to a system emergency including performing backups, preparing critical facilities, and appropriately detailed migration plans that can be used to facilitate continuity of operations in the event of an emergency and recovering from a disaster.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee is responsible for leading compliance activities that bring Hardin County General Hospital into compliance with regulatory requirements in areas such as:

- Data backup
- Disaster recovery
- Emergency mode operations
- Testing and revision
- Application and data criticality analysis

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will develop contingency plan documents to identify core activities in the areas of Data Backup, Disaster Recovery, Emergency Mode Operation, Testing and Revision, and Applications and Data Criticality Analysis.

Hardin County General Hospital will develop and implement a contingency plan to ensure the confidentiality, integrity, and availability of sensitive information during and after an emergency.

The core objectives of contingency planning include the capability to:

- Restore operations at an alternate site (if necessary)
- Recover operations using alternate equipment (if necessary)

- Perform some or all of the affected business processes using other means

The contingency plan will be developed for the entire enterprise. The contingency plan must address IT system components such as:

- Local, wide area and wireless networks including Internet access (if critical to the operation of the business)
- Server systems such as file, application, print and database
- Web sites
- Security systems such as firewalls, authentication servers, and intrusion detection
- Desktop, laptop, PDA systems

Hardin County General Hospital will follow the recommendations of The National Institute of Standards and Technology (NIST) in the area of contingency planning. The NIST recommends following seven key steps to address the requirements of contingency planning. These seven key steps for contingency planning are:

1. Develop the contingency policy objective statement
2. Conduct a Business Impact Analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Create the contingency plan
6. Conduct testing and training
7. Review and maintenance

Let us review the steps to better understand how we may be able to meet contingency planning requirements.

***Step 1: Contingency Policy Objective Statement***

The first step for the organization to address the requirements associated with contingency planning is to very clearly define the contingency planning policy. The core objective of the policy statement is to establish the organizational framework and responsibilities for contingency planning. NIST recommends that the contingency policy address the following topics:

- Roles and responsibilities
- Scope of policy with respect to systems/platforms and organizations functions subject to contingency planning
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Frequency of backups and storage of backup media

***Step 2: Business Impact Analysis (BIA)***

One of the critical steps in contingency planning is Business Impact Analysis (BIA). BIA helps to identify and prioritize critical Information Technology (IT) systems and components. IT systems may have numerous components, interfaces and processes. BIA enables a complete characterization of:

- System requirements
- Processes
- Interdependencies

As part of the BIA process, information is collected, analyzed and interpreted. The information provides the basis for defining contingency requirements and priorities.

The objective is to understand the impact of a threat on the business. The impact of the threat may be economical, operational or both. Questionnaires or survey tools may be used to collect the information.

BIA is performed at the beginning of disaster recovery and continuity planning to specifically identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. A key objective is to identify all critical systems that are required for the continuity of the business. Further, a determination of the time it would take to recover such systems in the event of a loss.

The critical steps for BIA include the need to:

1. Identify critical business functions
2. Identify disruption impacts and allowable outage times
3. Develop recovery priorities

***Step 3: Preventive Controls***

The BIA provides vital information regarding system availability and recovery requirements. It may be possible to mitigate some outage impacts identified in the BIA through preventive controls. The objective of preventive controls is to deter, detect, and/or reduce impacts to the system. Wherever possible, preventive controls are preferable to actions to recover the system after a disruption.

***Step 4: Recovery Strategies***

The objective of recovery strategies is to restore IT operations quickly and effectively following a disruption. A critical focus is to provide access to all sensitive information. Several factors will influence recovery strategy including cost, allowable outage time, security and integration with larger organizational-level contingency plans.

The choice for the recovery approach would depend on the incident, type of system and its operational requirements. Technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, Uninterruptible Power Supply (UPS), and mirrored systems should be considered when developing a system recovery strategy.

***Step 5: Development of Contingency Plan***

The contingency plan contains detailed roles, responsibilities, teams, and procedures associated with restoring critical systems following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements.

Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach. The NIST identifies five main components of the contingency plan. They are:

1. Supporting Information
2. Notification/Activation Phase

3. Recovery Phase
4. Reconstitution Phase
5. Plan Appendices

***Step 6: Testing and Training***

Testing of the plan is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures.

***Step 7: Review and Maintenance***

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan.

Procedures related to the Contingency Plan standard include:

- Data backup
- Disaster recovery
- Emergency mode operations
- Testing and revision
- Applications and data criticality analysis

## VI. DOCUMENTATION

- Business Impact Analysis (BIA) Report

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: DATA BACKUP PLAN** **Effective Date: 9/1/2012**
**Policy Number: HITECH 613** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Hardin County General Hospital will create and maintain exact, retrievable copies of sensitive information.

Hardin County General Hospital will ensure that sensitive data is backed up to disk, tape, or a combination of those technologies on a regular basis so as to minimize the loss of data in the event of an incident or disaster.

Hardin County General Hospital will ensure that backup media is periodically tested to ensure suitable quality and reliable data restoration.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for implementing the requirements of the data backup plan.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will develop the capability to secure the receipt, transport, and removal of:

- Hardware
- Software and
- And electronic media, such as diskettes, tapes, optical platters, and CD-ROMs

Hardin County General Hospital will document the following:

- Who has control of the hardware/software/or electronic media at all times
- Accountability, the ability to ensure that the actions of an entity can be traced back to that specific entity
- Data backup
- Data storage

- Disposal

In developing the backup schedule, the Information Technology Department, in conjunction with department supervisors, will consider factors such as:

- What data (systems, files, directories, and folders) should be backed up?
- How frequent are backups done?
- Who is responsible/ authorized to retrieve the media?

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: DISASTER RECOVERY PLAN** **Effective Date: 9/1/2012**
**Policy Number: HITECH 614** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to establish and implement as needed procedures to restore any loss of data.

The disaster recovery plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. A disaster recovery plan refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.

A disaster recovery plan provides a blueprint to continue business operations in the event that a catastrophe occurs. The disaster recovery plan must include contingencies for the period of time of the disaster and until the recovery plan can be completely implemented. The price for not developing a disaster recovery plan is that Hardin County General Hospital may find it difficult to continue to be in business or potentially suffer a significant loss.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Hardin County General Hospital will develop and maintain a Disaster Recovery Plan. The Compliance Team is to ensure the development of a Disaster Recovery Plan document.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for implementing the requirements of the Disaster Recovery Plan.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Hardin County General Hospital will assign final responsibility of security to one individual who will be referred to as the "Safety Officer."

The Compliance Committee is to ensure the development of a Disaster Recovery Plan document. This document typically includes the following sections:

1. Purpose
2. Scope
3. Assumptions
4. Team

5. Notification
6. Damage Assessment and Reporting
7. Activation
8. Recovery Operations
9. Return to Normal Operations

The *Purpose* section includes a statement describing the goal of the disaster recovery plan. The *Scope* section identifies the specific locations/sites and critical systems that are a part of the disaster recovery plan. The *Assumptions* section identifies the foundation that the plan is based on. The *Team* section identifies the Team lead for the activity as well as members of the IT organization and others that will be involved in the disaster recovery process.

The *Notification* section establishes the formal communication required to contact members to alert them of the incident. The *Damage Assessment and Reporting* section describes the process of analyzing the extent of damage to systems and sites and includes reports that identify recommendations for management. The *Activation* section describes the process to start disaster recovery activities. The *Recovery Operations* section describes the steps to recover critical systems and applications at the recovery site. This section would include information on data recovery based on the backed up data (Data Backup Plan). The *Return to Normal Operations* section describes the procedures for the team to follow for the full recovery of all data and enable a complete return to normal processing of all business functions.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: EMERGENCY MODE OPERATION PLAN** **Effective Date: 9/1/2012**
**Policy Number: HITECH 615** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in an emergency mode, as defined below.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Hardin County General Hospital Safety Officer must consider identifying the levels of emergencies and associated responses. The Safety Officer must develop specific components of the Emergency Mode Operation Plan, maintain those components, and periodically test the plan.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Safety Officer will be responsible for implementing the requirements of the Emergency Mode Operation Plan.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

The Safety Officer must consider identifying the levels of emergencies and associated responses. This may be based on the magnitude of the incident or disaster. For example:

- Level 1 Emergency may relate to a loss of business function or a specific part of a location/site.
- Level 2 Emergency may be based on an incident impacting multiple business functions or multiple locations/sites.
- Level 3 Emergency may be based on a significant disruption to several business functions or substantial damage at one or more locations/sites.

The specific components of an emergency mode operation plan must include:

- Identification of crisis management team members throughout the organization who will address strategic response of the organization in an emergency.
- Identification of support team members who will address tactical response of the organization in an emergency.
- Identification of a command center or other specifically designated facility to be utilized during emergency mode operation.

- Process for acquisition of additional human resources with applicable skill sets if current human resources are geographically restricted.
- Procedures and checklists to provide for the orderly transition and restoration of normal business operations (e.g., moving from the impacted site to the alternate site).
- Coordination of available critical facilities for alternate processing and business workspace for continuing operations in the event of an emergency.
- Communication plan for internal employees as well as external business partners and other stakeholders that addresses essential issues (e.g., Human Resources, Business Status and Financial concerns).
- Procedures to ensure that health and safety issues are addressed.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: WORKSTATION USE POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 616** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to 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 sensitive information.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information, such as sensitive information, by Hardin County General Hospital. In addition, this policy applies to all workstations and other computing devices owned or operated by Hardin County General Hospital and any computing device allowed to connect to Hardin County General Hospital's internal network.

Hardin County General Hospital will ensure that workstations and other computing devices are being used for work related purposes only.

All Hardin County General Hospital workstations will be utilized in a secure, approved manner, by authorized personnel only, and in such a way that the confidentiality, integrity, and availability of EPHI is not jeopardized.

Hardin County General Hospital will ensure that access is not permitted to Hardin County General Hospital workstations by individuals that are not authorized members of the Hardin County General Hospital workforce.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for ensuring the implementation of this policy.

## IV. EQUIPMENT

Workstations and computing devices owned by Hardin County General Hospital.

## V. PROCEDURES

### INFECTION CONTROL: N/A

The workstations and other computing devices at Hardin County General Hospital are to be used for work related purposes only. This includes, but is not limited to, Internet and Web access as well as the use of e-mail at Hardin County General Hospital. Workforce members should not expect any level of privacy as their activities, e-mails, files, and logs may be viewed at any time by the Compliance Committee or other members of management in support of this and other policies and procedures.

Hardin County General Hospital may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems.

Hardin County General Hospital will implement reasonable and appropriate measures to secure its computing devices could be used to access sensitive information. These measures will include, but are not limited to the following:

- All user and administrator accounts must be protected by some form of authentication. If passwords are used, they must follow the guidelines set forth in the Authentication Policy.
- All users accessing Hardin County General Hospital computing devices must have and use a unique user ID as set forth in the Authentication Policy.
- Procedures must be maintained that implement security updates and software patches in a timely manner.
- Procedures must be maintained that require users to run an up-to-date anti-virus program on all computing devices at Hardin County General Hospital.
- All unnecessary and unused services (or ports) must be disabled
- Measures will be taken to physically protect computers that are located in public areas and portable computers such as laptops and PDAs that can be taken off the premises.
- Computers located in public areas will be situated as to block unauthorized viewing and/or will have screen savers that black out the screen.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: WORKSTATION SECURITY POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 617** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement physical safeguards for all workstations that access sensitive information and to restrict access to authorized users.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Hardin County General Hospital. In addition, this policy applies to all workstations and other computing devices owned or operated by Hardin County General Hospital and any computing device allowed to connect to Hardin County General Hospital's internal network.

Hardin County General Hospital will implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users only.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

All individuals identified in the scope of this policy are responsible for:

- Using Hardin County General Hospital computing devices only for work related purposes
- Following all procedures implemented by the Compliance Committee related to this policy.

The Hardin County General Hospital Compliance Committee is responsible for:

- Maintaining procedures required to support this policy
- Supporting and ensuring compliance by workforce members

## IV. EQUIPMENT

Workstations and computing devices owned by Hardin County General Hospital.

## V. PROCEDURES

### INFECTION CONTROL: N/A

All members of the workforce will be trained on the appropriate and authorized use of workstations as part of the security awareness training.

Workstations will be positioned such that the monitor screens and keyboards are not within view of unauthorized individuals.

Users will logoff prior to leaving the workstation. Users will store any written passwords in secure locations only – under no circumstance must any password information be accessible on the workstation or its vicinity.

Workstations must be labeled to identify function and location and assist with compliance with access control procedures.

All workstations must be operated in a manner that ensures:

- Confidentiality of sensitive information.
- Employment of a password protected screen saver and/or workstation locking mechanism when the workstation is unattended.
- Proper log off and shut down of workstations at the end of the business day.
- Routine back up of all critical data.
- Virus scanning of media prior to use on any workstation.
- Only Information Technology Department approved software may be used on Hardin County General Hospital's systems.
- Workstations and said software is used in accordance with contract agreements and copyright laws.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: DEVICE AND MEDIA CONTROLS** **Effective Date: 9/1/2012**
**Policy Number: HITECH 618** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, and the movement of these items within a facility.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Hardin County General Hospital will ensure compliance with the Device and Media Controls standard (164.310(d)(1) and its associated implementation specifications of disposal, media re-use, accountability and data backup and storage.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for ensuring the implementation of the requirements of this policy.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Only authorized personnel will have access to sensitive information. A backup copy of all sensitive information and other critical software and applications will be stored in a secure location. A secure log will be maintained to document the disposal of any sensitive information.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: DISPOSAL POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 619** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement policies and procedures to address the final disposition of sensitive information and/or the hardware or electronic media on which it is stored.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Hardin County General Hospital will ensure that the master inventory list is appropriately updated upon the disposal of components containing sensitive information.

Hardin County General Hospital will ensure that the disposal of all sensitive information is conducted securely and that the destruction of the information is permanent.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for ensuring the implementation of the requirements of the Disposal Policy.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Hardin County General Hospital will ensure that prior to disposal either the data will be securely overwritten or physically destroyed and that such steps taken will be documented. Hardin County General Hospital will ensure that the data is permanently and securely destroyed in such a manner that it cannot be reassembled or recovered by any process currently available.

Hardin County General Hospital will ensure that all labels have been removed from such data to be disposed.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: AUTOMATIC LOGOFF POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 620** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

This policy applies to Hardin County General Hospital in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Hardin County General Hospital will configure all systems that support automatic logoff to require logoff after a predetermined period of time. If systems do not support automatic logoff capabilities, Hardin County General Hospital will request those capabilities from the appropriate vendor and document all vendor responses.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for ensuring the implementation of the Automatic Logoff Policy.

## IV. EQUIPMENT

Workstations and computing devices owned by Hardin County General Hospital.

## V. PROCEDURES

### INFECTION CONTROL: N/A

Hardin County General Hospital will maintain procedures for Automatic Logoff of systems that contain sensitive information after a period of inactivity. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the system is located.

Hardin County General Hospital will periodically inspect systems to ensure that the automatic session logoff capability is configured correctly.

If systems do not support automatic logoff capabilities, Hardin County General Hospital will request those capabilities from the appropriate vendor and document all vendor responses in writing.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: ENCRYPTION AND DECRYPTION POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 621** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement a mechanism to encrypt and decrypt sensitive information such as patient health information or personal identification information.

The Encryption Policy is intended to assist employees of Hardin County General Hospital when making a decision about the use of encryption technologies as a method of protecting data stored on systems that process sensitive information.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Hardin County General Hospital. More specifically, this policy applies to employees of Hardin County General Hospital that have the authority to evaluate, purchase (or develop), and implement systems that store or process sensitive information.

Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Hardin County General Hospital will identify systems that require sensitive information to be encrypted.

Hardin County General Hospital will identify members of the workforce, processes, and devices that require encryption capabilities and will implement those capabilities and test their proper functioning.

Hardin County General Hospital will only provide encryption keys to members of the workforce whose job role requires knowledge of encryption keys.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for ensuring the implementation of the Encryption and Decryption Policy.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Hardin County General Hospital will identify systems that require sensitive information to be encrypted.

Hardin County General Hospital will identify members of the workforce who require encryption capabilities.

Hardin County General Hospital will need to balance the challenge of protecting "data at rest" against the increase in security technology complexity and administrative overhead including performance considerations and usability.

Hardin County General Hospital will seriously review the viability of securing critical database, file servers as well as sensitive information on mobile devices such as laptops and PDAs.

Data at rest will follow NIST Special Publications 800-111 wherever possible. Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption.

Symmetric cryptosystem key lengths must be at least 128 bits.

Asymmetric crypto-system keys must be of a length that yields equivalent strength.

Hardin County General Hospital key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Information Technology Department.

Hardin County General Hospital will test encryption and decryption capabilities of products and systems to ensure proper functionality.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: NETWORK SECURITY POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 622** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to secure communication devices and data on the Hardin County General Hospital network.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information.

Hardin County General Hospital will evaluate the need for secure communication on all networks, public and private, that are utilized to transmit Hardin County General Hospital sensitive information.

Where secure communications are required, technology and processes will be put in place to ensure the confidentiality and integrity of sensitive information.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee will be responsible for ensuring that network protocols are configured securely.

## IV. EQUIPMENT

NA

## V. PROCEDURES

### INFECTION CONTROL: N/A

Where secure communications are required, technology and processes will be put in place to ensure the confidentiality and integrity of sensitive information.

The standard for network protocols in the Hardin County General Hospital infrastructure is TCP/IP.

Hardin County General Hospital will:

- Use encryption as much as possible to protect data
- Use firewall(s) to secure critical segments
- Disable all services that are not in use or services that have use of which you are not sure
- Use wrappers around all services to log their usage as well as to restrict connectivity

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: EMAIL SECURITY POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 623** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose of this policy is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Hardin County General Hospital. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Hardin County General Hospital will identify whether sensitive information is permitted to be transmitted over email, and secure all email transmissions of sensitive information whenever it is permitted.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

All individuals identified in the scope of this policy are responsible for:

- Abide by the terms and guidelines set forth by this policy

The Compliance Committee is responsible for:

- Evaluating, on a periodic basis, emerging encryption solutions for email and implementing them when one is found the meets the criteria described in the policy section of this document
- Maintaining procedures and forms in support of this policy
- Monitoring and enforcing workforce compliance with this policy

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Hardin County General Hospital recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages. Hardin County General Hospital will evaluate emerging encryption solutions for email and implement them when one is found that is:

- Technically sound
- Reasonable to implement and use by workforce members
- Financially reasonable

Until a workable encryption mechanism is implemented, Hardin County General Hospital will utilize the following guidelines regarding sending sensitive information via email:

- Emails containing sensitive information are permitted only when both the sender and receiver are members of Hardin County General Hospital's workforce and the e-mail stays within the confines of Hardin County General Hospital's local network. That is, both email addresses must end with ilhcgh.org. When sending sensitive information via email, care should be taken to send only the minimum necessary.
- Emails containing sensitive information may not be sent to any other person outside of Hardin County General Hospital's network.

Hardin County General Hospital provided e-mail systems are intended for official and authorized purposes only. E-mail messages are considered by Hardin County General Hospital to be company property. Therefore, e-mail equipment operated by or for Hardin County General Hospital staff are subject to the same restrictions on their use as any other company furnished resource provided for use by members of the workforce.

Electronic information about an individual, such as a client or a patient, in an organized set of records, should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.

E-mail system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate Hardin County General Hospital management officials. However, Hardin County General Hospital officials will have access to e-mail messages whenever there is a legitimate purpose for such access, e.g., technical or administrative problems.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: REMOTE ACCESS POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 624** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to Hardin County General Hospital's enterprise infrastructure to a reasonable and appropriate level.

This policy applies to Hardin County General Hospital in its entirety, including all facilities and systems that process sensitive information. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

Hardin County General Hospital will take all reasonable and appropriate steps to ensure the secure and authorized use of all remote access capabilities and solutions.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee has the responsibility to ensure that all remote access connections are used based on policy requirements. The Compliance Committee must review related log files from key systems on a regular basis.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

The Hardin County General Hospital remote access infrastructure must follow these guidelines:

- It is the responsibility of Hardin County General Hospital employees, contractors, vendors and agents with remote access privileges to Hardin County General Hospital corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Hardin County General Hospital.
- General access to the Internet for recreational use by immediate household members through the Hardin County General Hospital network on personal computers is permitted for employees that have flat-rate services. The Hardin County General Hospital employee is responsible to ensure the family member does not violate any Hardin County General Hospital policies, does not perform illegal activities, and does not use the access for outside business interests. The Hardin County General Hospital employee bears responsibility for the consequences should the access be misused.
- Secure remote access must be strictly controlled. Control will be enforced by using strong passwords.
- At no time should any Hardin County General Hospital employee provide their login or e-mail password to anyone, not even family members.

- Hardin County General Hospital employees and contractors with remote access privileges must ensure that their Hardin County General Hospital owned or personal computer or workstation, which is remotely connected to Hardin County General Hospital corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Hardin County General Hospital employees and contractors with remote access privileges to Hardin County General Hospital's corporate network must not use non-Hardin County General Hospital e-mail accounts (for example, Hotmail, Yahoo, AOL), or other external resources to conduct Hardin County General Hospital business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the Hardin County General Hospital network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by the Information Technology Department.
- All hosts that are connected to Hardin County General Hospital internal networks via remote access technologies must use the most up-to-date anti-virus, this includes personal computers.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the Hardin County General Hospital production network must obtain prior approval from the Information Technology Department.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: PORTABLE DEVICES POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 625** **Med Staff:**
**Regulation: HITECH** **Admin:**

## I. POLICY

The purpose is to secure the use of portable devices used by members of the workforce.

This policy applies to all members of the workforce, including volunteers. The policy applies to all types of portable devices, including and not limited to CDs, DVDs, flashdrives, laptops, notebooks, PDAs, smart phones, and any other mobile device that is capable to storing or transmitting sensitive information.

Hardin County General Hospital will ensure that wherever and whenever the use of portable devices is deemed necessary, these devices will be appropriately secured and used only by properly authorized members of the workforce.

Hardin County General Hospital will ensure that all portable devices will be used according to the guidelines defined in this policy.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

Employees are responsible for the security of portable devices they use for work. Special care should be taken to ensure that sensitive information is not compromised.

The Compliance Committee will ensure that key elements of this policy may be included in any training provided to all members of the workforce. The Information Technology Department may include elements of this policy as security reminders sent to members of the workforce. If encryption software is installed on portable devices or if strong password controls are implemented then members of the workforce must be trained in this area.

The Information Technology Department is responsible for conducting random audits of portable systems to check for unauthorized or unsecured files.

## IV. EQUIPMENT

Portable systems and computing devices owned by Hardin County General Hospital.

## V. PROCEDURES

### INFECTION CONTROL: N/A

Confidential or sensitive data must be accessed only on server systems. Sensitive information may only be stored on portable systems if appropriate encryption software authorized by the Information Technology Department is installed on the device. Any information stored on the portable system must be saved only in those folders that keep information encrypted.

Strong password controls must be implemented for all users of portable devices. This includes requirements for minimal password length (such as 8 characters, alphanumeric) and frequency of password changes (such as every 90 days).

When working on portable devices from a remote location, including from home, only secure connections must be used to access sensitive information. If wireless communication is used with portable devices then the device must be configured as defined by the Information Technology Department to ensure use of secure protocols.

Backups of information from portable devices must be conducted regularly and stored securely.

Employees must logoff and shut down portable devices with sensitive data before leaving the work space. Protection against malicious software should be in place and be kept up to date.

Devices must be configured to automatically logoff users according to Automatic Logoff Policy, HITECH 620.

Portable devices must not be left unattended. When not in use, portable devices should be locked away or special locks should be used to secure the equipment.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: VIRTUAL PRIVATE NETWORK POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 626** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose of this policy is to implement security measures sufficient to reduce the risks and vulnerabilities of Hardin County General Hospital's VPN infrastructure to a reasonable and appropriate level.

This policy applies to Hardin County General Hospital in its entirety, including all facilities and systems that process sensitive information.

Hardin County General Hospital will ensure the VPN is appropriately secured at all times, and will adhere to the requirements defined in this policy.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee has the responsibility to ensure that all VPN end systems such as laptops and desktops, are deployed and used based on policy requirements. The Information Technology Department must review log files from VPN devices such as concentrators and other systems on a regular basis.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Hardin County General Hospital VPN infrastructure must follow these guidelines:

- Members of the workforce with VPN privileges must ensure that unauthorized users are not allowed access to Hardin County General Hospital internal networks.
- VPN use is to be controlled using either a one-time password authentication such as a token device or a strong password solution.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic must be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by Hardin County General Hospital network operational groups.
- All computers connected to Hardin County General Hospital internal networks via VPN or any other technology must use the most up-to-date anti-virus software; this includes personal computers.
- VPN users are automatically disconnected from Hardin County General Hospital network after fifteen minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computers that are not Hardin County General Hospital-owned equipment must configure the equipment to comply with Hardin County General Hospital VPN and other policies.
- Only approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Hardin County General Hospital network, and as such are subject to the same rules and regulations that apply to Hardin County General Hospital-owned equipment; in other words, their machines must be configured to comply with Hardin County General Hospital Security Policies.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: WIRELESS SECURITY POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 627** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of Hardin County General Hospital's wireless infrastructure to a reasonable and appropriate level.

This policy applies to Hardin County General Hospital in its entirety, including all facilities and systems that process sensitive information.

Hardin County General Hospital will operate all wireless networks in a secure manner so as to ensure the confidentiality, integrity, and availability of all sensitive information transmitted over wireless networks.

Hardin County General Hospital will ensure that all wireless devices are configured and operated according to the requirements set forth in this policy.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

The Compliance Committee has the responsibility to ensure that all wireless end systems such as laptops and PDAs, as well as all APs are deployed based on policy requirements. The Compliance Committee may review log files from APs and other systems on a regular basis. The Compliance Committee may send reminders to all employees about wireless network security.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Hardin County General Hospital wireless infrastructure must follow these guidelines:

***Design***

- Configure a firewall between the wireless network and the wired infrastructure.
- Ensure that 128-bit or higher encryption is used for all wireless communication.
- Fully test and deploy software patches and updates on a regular basis.

***Access Points (AP)***

- Maintain and update an inventory of all Access Points (AP) and wireless devices.
- Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
- Place APs in secured areas to prevent unauthorized physical access and user manipulation.
- The default settings on APs, such as those for SSIDs, must be changed.

- APs must be restored to the latest security settings when the reset functions are used.
- Ensure that all APs have strong administrative passwords.
- Enable user authentication mechanisms for the management interfaces of the AP.
- Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
- Turn on audit capabilities on AP; review log files on a regular basis.

***Mobile Systems***

- Install anti-virus software on all wireless clients.

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: DATA BREACH DISCOVERY, MANAGEMENT AND NOTIFICATION POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 628** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

The purpose of the Data Breach Discovery Policy is to provide guidance to the employees of Hardin County General Hospital in defining and identifying potential security breaches of protected information, such as Protected Health Information (PHI), personal information or other confidential information. Through proper education and preparedness Hardin County General Hospital can better protect all of its confidential and sensitive information.

The purpose of the Data Breach Management Policy is to assist employees responsible for managing breach related activities of Hardin County General Hospital when making decisions after a data breach has been identified. This policy is designed to minimize the loss and destruction of data, mitigate the weakness that was exploited and restore all computing and other impacted services to Hardin County General Hospital.

The Data Breach Notification Policy is intended to assist employees responsible for addressing breach notifications of Hardin County General Hospital when making decisions regarding the notification actions required after a breach of protected information is discovered.

This policy applies to all Hardin County General Hospital workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Hardin County General Hospital. All workforce members are responsible for the security of protected information.

Hardin County General Hospital will employ policies, technologies, and education to identify security breaches.

Hardin County General Hospital will ensure that if a data breach is discovered the steps laid out in this policy will be followed in order to prevent further damage, assess the severity of the breach, and manage all associated breach related activities.

Hardin County General Hospital will notify persons and organization that have been impacted by a data breach.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

All workforce members are responsible for:

- Understanding and following all security related policies and procedures

The Compliance Officer is responsible for:

- Ensuring all workforce members understand and follow security related policies and procedures

Compliance Committee is responsible for:

- The proper management of the security incident

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

DISCOVERY

Hardin County General Hospital will employ policies, technologies, and education to identify security breaches.

***A breach is defined as:***

The unauthorized acquisition, access, use, or disclosure of protected information as defined below, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Breach does not include:

(i) any unintentional acquisition, access, or use of protected information by an employee or individual acting under the authority of a covered entity or business associate if
   a. such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and
   b. such information is not further acquired, accessed, used, or disclosed by any person; or

(ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and

(iii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

(iv) Information that has been rendered unusable, unreadable, or indecipherable according to the definition below.

*Policies and Procedures:*

Hardin County General Hospital will implement policies and procedures to protect against and identify data breaches. The policies will minimally include:

- Disposal Policy HITECH 619
- Workforce Security Policy HITECH 606
- Risk Analysis Policy HITECH 602
- Security Incident Procedures HITECH 610
- Response and Reporting Policy HITECH 611
- Encryption and Decryption Policy HITECH 621

*Technology:*

The technology infrastructure at Hardin County General Hospital will be monitored for data breaches utilizing standard industry technologies including but not limited to the following:

- Firewall

- Virus Protection Systems
- Malware Protection Systems

*Education:*
Hardin County General Hospital business users and staff will be educated in standard breach identification and prevention methodologies; including but not limited to the following:

- Suspicious PC activity
- Suspicious emails regarding protected information
- Virus, Malware and Security software alerts
- Phishing methods

If a breach of Protected Information is discovered the person making the discovery will notify the Compliance Officer.

The Compliance Committee will as necessary execute the Security Incident Procedures Policy, Response and Reporting Policy, Data Breach Management Policy, the Data Breach Notification Policy and other policies as appropriate.

Persons will report to the Compliance Committee any improper disposal of Protected Information utilizing the Disposal Policy HITECH 619 as a guide.

DATA BREACH MANAGEMENT
If a data breach is discovered at Hardin County General Hospital the following steps will be followed in order to prevent further damage, assess the severity of the breach, and manage all associated breach related activities.

- Once a breach has been identified, the Security Officer will assemble the Compliance Committee according to the Security Incident Procedures Policy HITECH 610, develop a response according to the Response and Reporting Policy HITECH 611, review the breach details and develop an appropriate response to prevent further data leakage, and assess the details of the breach.
- The Compliance Officer and the Compliance Committee will manage all phases of the process once a breach has been identified.
- The Compliance Officer and the Compliance Committee will keep Hardin County General Hospital leadership apprised of the situation.
- Priorities of the Compliance Officer and the Compliance Committee will be:
    - Stopping the data leakage
    - Mitigation of the weakness, that was exploited
    - Restoration of normal business
    - Notification of persons and businesses impacted as deemed appropriate
- The Compliance Officer and Compliance Committee may work with Hardin County General Hospital legal counsel to determine applicable state and federal laws that may be applicable to the incident; including by not limited to HIPAA, HITECH, and state breach notification laws.
- If any form of protected information; as defined in this policy, is at risk then the Compliance Officer and Compliance Committee are to enact the Breach Notification Policy.

- Forensic analysis of the breach is to begin immediately upon determination of the breach, unless law enforcement deems a delay is appropriate, or additional forensic support is required beyond the Hardin County General Hospital Compliance Committee.
- All meeting minutes, technical documentation, and hand written notes of the breach are to be compiled by the Compliance Officer or designee within 72 hours of the closure of the breach.
- Any systems that were compromised or targeted as part of an incident resulting in an investigation may be quarantined as determined by the Compliance Officer and Compliance Committee.
- Based upon the scope of the perceived threat the Security Officer and Compliance Committee will notify local law enforcement, the FBI Cyber Security Team for assistance, http://www.fbi.gov/contact/fo/fo.htm or the FBI Internet Crime Complaint Center (IC3) http://www.ic3.gov/default.aspx.

NOTIFICATION

Hardin County General Hospital will notify persons and organization that have been impacted by a data breach.

- The Compliance Officer will work with Hardin County General Hospital legal counsel to determine state and federal laws that may be applicable to the incident; including but not limited to HIPAA, HITECH, and state breach notification regulations
- The Compliance Committee will prepare any public notices
- Notifications will be made in the most expedient time possible and without unreasonable delay
- Notifications are to occur according to the requirements of HITECH for PHI (maximum of 60 days) or applicable state breach laws for Protected Information
- Notifications may be delayed at the request of law enforcement agencies as part of their investigation process
- Notifications may be delayed to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the impacted system
- Notifications will be made at no charge to the impacted individuals or organizations
- Method(s) of notification may vary according to the type of breach, severity of breach, and applicable laws and regulations therefore;
    - All breach notifications will be made according to HITECH standards; unless state regulations set more rigorous requirements. (ARRA - Sec 13402 – Notification in the Case of a Breach)
        - HITECH requires covered entities to notify individuals whose unsecured information has been breached
        - HITECH requires business associates to notify covered entities about breaches
        - HITECH requires that the covered entity notify individuals whose information has been breached within 60 days of discovery
        - HITECH requires written notification to affected individuals by mail and if urgent, by telephone
        - HITECH requires a conspicuous posting on the home page of the covered entity involved as determined by the Secretary of DHHS or in major print or broadcast media
        - HITECH requires breaches of over 500 affected individuals to be reported to media outlets and the Secretary of DHHS

HITECH requires breaches of less than 500 affected individuals to submit a log annually to the Secretary of DHHS

NOTIFICATION TO HHS
Hardin County General Hospital will notify persons and organization that have been impacted by a data breach, and require notification as determined by this policy. This policy will serve as guidance to determine if, when and how HHS is to be notified.

**To determine the required notification for HHS the following must be considered:**

**How soon to notify:**
- Were more than 500 persons impacted by the breach?
    - **Yes:** Notice to the Secretary of HHS must be provided **immediately**
    - **No:** Covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary of HHS documenting such breaches occurring during the year involved

**Who will notify:**
- The Compliance Officer will work with the Compliance Committee and the management team to develop and coordinate all communications.

**Methods to notify HHS:**
- On-line
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

- Letter via First Class mail (certified mail recommended):
  Secretary
  U.S. Department of Health and Human Services
  Office for Civil Rights
  Attention: HITECH Breach Notification
  Hubert H. Humphrey Building, Room 509F
  200 Independence Avenue, SW
  Washington, DC 20201

- Phone:
    - Contact the appropriate Regional Office of The Department of Health and Human Services Office for Civil Rights to discuss any details relative to specifics of a breach event:

**Region I - Boston (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont)**
Voice phone(617)565-1340
FAX (617)565-3809
TDD (617)565-1343

**Region II - New York (New Jersey, New York, Puerto Rico, Virgin Islands)**
Voice Phone (212)264-3313
FAX (212)264-3039
TDD (212)264-2355

**Region III - Philadelphia (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia)**
Voice Main Line (215)861-4441
Voice Hotline (800) 368-1019
FAX (215)861-4431
TDD (215)861-4440

**Region IV - Atlanta (Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee)**
Voice Phone (404)562-7886
FAX (404)562-7881
TDD (404)331-2867

**Region V - Chicago (Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin)**
Voice Phone (312)886-2359
FAX (312)886-1807
TDD (312)353-5693

**Region VI - Dallas (Arkansas, Louisiana, New Mexico, Oklahoma, Texas)**
Voice Phone (214)767-4056
FAX (214)767-0432
TDD (214)767-8940

**Region VII - Kansas City (Iowa, Kansas, Missouri, Nebraska)**
Voice Phone (816)426-7277
FAX (816)426-3686
TDD (816)426-7065

**Region VIII - Denver (Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming)**
Voice Phone (303)844-2024
FAX (303)844-2025
TDD (303)844-3439

**Region IX - San Francisco (American Samoa, Arizona, California, Guam, Hawaii, Nevada)**
Voice Phone (415)437-8310

**All notifications to HHS must contain the following items:**

- Notice of a breach shall include, to the extent possible, the following:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
    - The steps individuals should take to protect themselves from potential harm resulting from the breach.
    - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Data Breach Notification to HHS ECP-704, Attachment A:

Sample Breach Notice – (Specifics vary according to exact information breached)

[DATE]

[NAME], Secretary
U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

***Re: HITECH Breach Notification***

Dear Secretary:

<<Organization Name>> discovered on [DATE of Breach Discovery] that there was a breach unprotected patient information impacting [number of patients impacted] patients. [Brief description of breach including the type of data breached (SSN, DOB, Address, Acct Number, or Disability Code)].

<<Organization Name>> has taken the following steps to investigate the breach, mitigate losses, and protect against further breached. [Description of steps taken and planed]

<<Organization Name>> has notified all individuals utilizing the template letter attached (Attachment A)

Please contact me directly if you require any further information regarding this incident.

Respectfully,

Julie Parker, CEO
<<Organization Name>>
1234 Anystreet
Anywhere, IL 55555
E: Julie.Parker@anywhere.com
P: 555.555.5555
F: 777.777.7777

DATA BREACH NOTIFICATION TO PATIENT

Hardin County General Hospital will notify persons that have been impacted by a data breach, and require notification as determined by Data Breach Notification Policy. This policy will serve as guidance to determine if, when and how Patients are to be notified.

To determine the required notification for Patients the following must be considered:

**How soon to notify:**

- Within 60 days of discovery of the breach

**Who will notify:**

- The Compliance Officer will work with the Compliance Committee and the management team to develop and coordinate all communications.

**Methods to notify Patient:**

- Primary Method:
    - Letter via First Class mail or email if specified as preferred by the patient, to individuals impacted by breach:
        - (Sample Letter in Attachment A)
    - If individual is deceased then the above applies to their next of kin
    - Multiple notifications may be necessary as information becomes available

- Secondary Method:
    - In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under primary method, electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of Hardin County General Hospital or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

- Tertiary Method:
    - In any case deemed by Hardin County General Hospital to require urgency because of possible imminent misuse of unsecured protected health information Hardin County General Hospital, in addition to notice provided under Primary Method, may provide information to individuals by telephone or other means, as appropriate.

**All notifications to Patients must contain the following items:**

- Notice of a breach shall include, to the extent possible, the following:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

- The steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

Data Breach Notification to Patient, ECP-705, Attachment A:

*Salutation,*

We are writing to you because of a recent security incident at Hardin County General Hospital.

[*Describe what happened in general terms, specifically what kind of personal information was involved and dates of breach]*

*Hardin County General Hospital is taking these steps to secure your information [Steps being taken to investigate the data breach, mitigate losses and protect against future losses*.]

*[Include the following sections as appropriate]*

Because your [Social Security, credit card, banking] number was involved, and in order to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in the enclosed pamphlet from the FTC: TAKE CHARGE; Fighting Back Against Identity Theft.

Since your health information [*or insurance information, policy, plan number, or subscriber identification number*] was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from [*your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For more information about privacy protection steps and your medical privacy rights, we recommend you visit our web site www.ilhcgh.org

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated institution official or institution unit handling inquiries*] at [*toll-free phone number*].

Respectfully,

Julie Parker, CEO
<<Organization Name>>
1234 Anystreet
Anywhere, IL  55555
E: Julie.Parker@anywhere.com
P: 555.555.5555
F: 777.777.7777

Enclosure [FTC handbook: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf]

DATA BREACH NOTIFICATION TO MEDIA
Hardin County General Hospital will notify persons that have been impacted by a data breach, and require notification as determined by this Policy. This policy will serve as guidance to determine if, when and how the media is to be notified.

To determine the required notification for Media the following must be considered:

**How soon to notify:**
- Were more than 500 persons impacted by the breach?
    - **Yes:** Notice to prominent media outlets must be provided **immediately**
    - **No:** Notice to prominent media outlets is not required

**Who will notify:**
- The Compliance Officer will work with the Compliance Committee and the management team to develop and coordinate all communications.

**Methods to notify Media:**
- Primary Method:
    - Phone call to prominent media outlets.
        - Media Outlets can be located at the following web address: http://www.congress.org/congressorg/dbq/media/

**All notifications to prominent media outlets must contain the following items:**

- Notice of a breach shall include, to the extent possible, the following:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
    - The steps individuals should take to protect themselves from potential harm resulting from the breach.
    - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Data Breach Notification to Media, ECP-706, Attachment A:

[*Salutation*]

We are writing to your organization because of a recent security incident at Hardin County General Hospital and request that your organization assist us in providing public notice as part of the HITECH breach notification act.

[*Describe what happened in general terms, specifically what kind of personal information was involved and dates of breach]*

*Hardin County General Hospital is taking these steps to secure the individuals information [Steps being taken to investigate the data breach, mitigate losses and protect against future losses*.]

*[Include the following sections as appropriate]*

Because a [Social Security, credit card, banking] number was involved, and in order to protect each individual from the possibility of identity theft, we recommend that each individual places a fraud alert on their credit files and order copies of their credit reports by following the recommended privacy protection steps outlined in the enclosure. Each individual should check their credit reports for any accounts or medical bills that they do not recognize. If any individual finds anything suspicious, follow the instructions found on the FTC web site: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm or on the Hardin County General Hospital web site: www.ilhcgh.org

Since your health information [*or insurance information, policy, plan number, or subscriber identification number*] was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from [*your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

Each individual should keep a copy of this notice for their records in case of future problems with their medical records. They may also want to request a copy of their medical records from their [*provider or plan*], to serve as a baseline. For more information about privacy protection steps and individual medical privacy rights, we recommend individuals visit our web site www.ilhcgh.org

We regret that this incident occurred and want to assure everybody we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should anybody need any further information about this incident, please contact [*name of the designated institution official or institution unit handling inquiries*] at [*toll-free phone number*].
Please contact our media relations department at (555) 555-1212 to further review this incident.

Respectfully,

Julie Parker, CEO
<<Organization Name>>
1234 Anystreet
Anywhere, IL  55555
E: Julie.Parker@anywhere.com
P: 555.555.5555
F: 777.777.7777

Enclosure [FTC handbook: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf]

## VI. DOCUMENTATION

NA

**HARDIN COUNTY GENERAL HOSPITAL**
**HOSPITAL-WIDE POLICY**

**Title: SOCIAL MEDIA POLICY** **Effective Date: 9/1/2012**
**Policy Number: HITECH 629** **Med Staff:**
**Regulation: HITECH ACT of 2009** **Admin:**

## I. POLICY

Hardin County General Hospital recognizes that the use of the internet has many benefits for Hardin County General Hospital and its staff. The internet and email make communication more efficient and effective. Therefore, staff is encouraged to use the internet and email appropriately.

Today, social media encompasses a broad sweep of online activity, all of which is track-able and traceable. These networks include not only the blogs you write and those in which you comment, but social networks such as Facebook and MySpace; professional networks such as LinkedIn; the live blogging tool Twitter; photo-and video-sharing sites like flickr and YouTube; and social bookmarking such as Digg and Delicious. Every day, it seems, new online tools and technical advances introduce new opportunities to build a "virtual" footprint.

With the rapid growth and application of social media, Hardin County General Hospital recognizes the need to have a policy which ensures that staff who use social media, either as part of their job or in a personal capacity, have guidance as to the organization's expectations where the social media engagement is about Hardin County General Hospital, its services, Hardin County General Hospital staff, Hardin County General Hospital patients, its competitors, its vendors and/or business-related individuals or organizations.

This policy applies to Hardin County General Hospitalin its entirety, including all workforce members. Hardin County General Hospital's "3 Rs of electronic engagement" are, therefore, "guardrails" designed to protect the interests of Hardin County General Hospital and staff. In brief, the 3 Rs ask that when using the internet, e-mail, engaging in social media or any form of electronic communications, you be clear about whom you are representing, you take responsibility for ensuring that any references to Hardin County General Hospital are factually correct and accurate and do not breach confidentiality requirements, and that you show respect for the individuals and communities with which you interact.

The intent of this policy is to maintain effective e-communications that are consistent with the Hardin County General Hospital Commitment and Beliefs and Workforce Standards. These guidelines are applicable whether or not you are using Hardin County General Hospital tools to IM, text or e-mail, or when using the internet as part of your job or when using the internet for personal social networking that involves Hardin County General Hospital references.

## II. DEFINITIONS

NA

## III. RESPONSIBILITY

- While utilizing Hardin County General Hospital provided tools disclose that you are employed by Hardin County General Hospital and be clear about what department or service you are representing and what are your role and accountabilities.

- Write what you know, write in the first person and make sure you write and post about your areas of expertise, especially as it relates to Hardin County General Hospital.
- You may not disclose any confidential or proprietary information about Hardin County General Hospital, its patients, affiliates, vendors or suppliers.
- Hardin County General Hospital logos may not be utilized without written consent (contact Management).
- Personal blogs should have clear disclaimers that the views expressed by the author in the blog are the authors alone and do not represent the views of Hardin County General Hospital. Make your writing clear that you are speaking for yourself and not on behalf of the organization.
- While you are at work, please refrain from online activities that don't bring value to Hardin County General Hospital. Think of your personal time online as you think of personal phone calls or emails. If not required for your particular job role/activity, online activities should be limited to non-worked time (considered as before a shift begins, during breaks or meal periods or after a shift ends). Social media activities should not interfere with work commitments.
- Remember that the internet is not anonymous, nor does it forget. Everything written on the web can be very easily traced back to its author one way or another. Information is backed up often and repeatedly and posts in one forum are usually replicated in others through tracebacks, reposts or references.
- You are responsible for what you post. You are personally responsible for any of your online activity conducted with the Hardin County General Hospital email address, and/or which can be traced back to the organization's domain, and/or which uses organization assets. The ihcgh.org address attached to your name implies that you are acting on the organization's behalf.
- Do not use or disclose any patient identifiable information, or any patient scenarios of any kind on any social media.
- If it gives you pause, pause. If you're about to send an email or post a blog, for example, and the message makes you even the slightest bit uncomfortable, don't shrug it off and hit "send." Take a minute to review these guidelines and try to figure out what's bothering you, then fix it.
- Remember confidentiality when using cell phones within the organization. An overheard cell phone conversation or an indiscreet text message could put the organization at risk.

Do not presume that your activities on the internet are private or your business alone. Outside the workplace, your rights to privacy and free speech protect online activity conducted on your personal social networks with your personal email address. However, what you publish on such personal online sites should never be attributed to Hardin County General Hospital and should not appear to be endorsed by or originated by Hardin County General Hospital. This means, whether working on Hardin County General Hospital equipment during business hours, or on personal technology tools at home after work, the posting of text, photos, or videos about the organization, Hardin County General Hospital staff, Hardin County General Hospital patients, products or services, etc., without express permission from your Director may be considered a violation of this policy. If you choose to list your work affiliation on a social network, then you should regard all communications on that network as you would in a professional network. Online lives are ultimately linked, whether or not you choose to mention Hardin County General Hospital in your personal online networking activity.

Staff is obligated to report suspected violations of this policy to their Director, Hardin County General Hospital Compliance Officer, IT or Human Resources.

- When activity by an individual is seen as in conflict with the content and intent of this policy the Department Director, upon investigation and confirmation of such conflict, will evaluate options including cessation of the identified activity, loss of internet availability or initiating the Sanction Policy, up to and including dismissal.

## IV. EQUIPMENT

NA

## V. PROCEDURES

**INFECTION CONTROL: N/A**

Every e-mail transmitted by an individual reflects on the organization's credibility and the professionalism of the writer. Adherence to the basic rules of Hardin County General Hospital netiquette below will alleviate problems and help cast you and Hardin County General Hospital in a favorable light.

- Beware of hidden readers. If confidentiality is an issue, don't use e-mail. You may intend to send a message to one person, but an inaccurate keystroke could land the email on dozens or hundreds of readers' screens.
- Write as though mom were reading. Don't take e-mail too casually. Write your message as if your Director, the media or your mom were reading it.
- Keep all the organization's policies in mind. A policy is a policy. You are obligated to adhere to the organization's policies, whether working on Hardin County General Hospital provided tools or off site on personal tools.
- Don't use email to let off steam. Don't take the chance of sending a hastily written message that could worsen an already difficult decision.
- Control the urge to flame. An e-mail flame is a message that is hostile, blunt, rude, insensitive, or obscene. Flames and the obscene and abusive language that feed them have no place at Hardin County General Hospital.
- Respect others' time. Do not use the organizational system to send or forward spam, non-business related messages, or personal correspondence.
- Never reply to spam. If you are on the receiving end of spam, do not reply to the "unsubscribe" option. Your reply merely confirms your e-mail address and encourages the sender to sell your address to other spammers.
- Don't post your business e-mail address on a personal website. Spambots automatically search the web for e-mail addresses for use by spammers.
- Don't mail to the world. Send emails only to readers with a legitimate need for the information. Mail to group list only when it is appropriate for everyone on the list to receive the message. Staff is prohibited from sending organizational-wide e-mail messages to all staff without prior approval of the individual's Director, NET member and IT. If you do not wish a message to be forwarded once received, put that in the email so the recipient is aware.
- Copy with care. Sending a carbon copy (CC) or blind carbon copy (BCC) to a recipient who doesn't need to read your message wastes everyone's time.
- Don't oversell your message. Reserve the urgent classification for messages that demand immediate attention.

- Ask permission to forward material. Avoid infringement on copyright laws on publications to which you may subscribe. Seek authorization from the original sender before sending out material.
- Consider e-mail limitations. E-mail may be the best way to deliver a message quickly but is not necessarily the best route to a quick reply. For an immediate response to a pressing issue don't rely on e-mail. Instead, pick up the phone or schedule a face-to-face meeting.

Know who sees your message. Remember that when you post something on a friend's Facebook page, you are sending it to all of their friends as well. There are few to no boundaries in this type of activity.

Cell Phones and Texting

- Staff may use cell phones and texting to communicate during non-work hours (breaks, meal periods) and during emergencies.
- Cell phone conversations or texting should not occur in any area where patients or visitors are present.
- Cell phones should be turned off or set to silent or vibrate mode during meetings, conferences and in other locations where incoming calls may disrupt normal workflow.
- Directors reserve the right to request that an individual provide his/her cell phone bills and usage reports for calls made during the working hours of the person to determine if use is excessive.

Property Rights and Confidentiality

- All information created, transmitted, acquired, downloaded, or uploaded via the organization's network and internet or intranet is the property of Hardin County General Hospital.
- Internal and external e-mail messages are considered business records and may be subject to discovery in the event of litigation. All electronic communications produced through the utilization of Hardin County General Hospital tools or internet access, including internal and external emails, may be subject to disclosure to a third party.
- E-mail is not guaranteed to be private or confidential. All electronic communications are Hardin County General Hospital property. Therefore, Hardin County General Hospital reserves the right at any time to examine, monitor, and regulate e-mail messages, directories and files, as well as internet usage.

## VI. DOCUMENTATION

NA