RANKIN COUNTY HOSPITAL DISTRICT	
DEVICE AND MEDIA CONTROL POLICY	
# of Pages: 1 of 1	

POLICY

It is the policy of **Rankin County Hospital District** to manage the receipt and removal of hardware and software that contain electronic protected health information (PHI) into and out of the organization and the movement of electronic PHI within the organization.

PROCEDURES

I. DISPOSAL — POLICY & PROCEDURE STANDARDS

A. The Security Officer shall be responsible for implementing procedures for the disposal of old data electronic PHI.

B. All employees shall dispose of old data containing electronic PHI on all media (tapes, diskettes, hard drives, etc.) by physically destroying the media in such a manner that it can never be used again.

C. The Security Officer shall implement documented purge criteria for electronic PHI.

D. The Security Officer is responsible for disposing of old data and electronic EPHI. The Security Officer shall document periodic review and update of data disposal processes.

11. MEDIA RE-USE — POLICY & PROCEDURE STANDARDS

A. The Security Officer is responsible for removing any electronic PHI from all media before reuse

B. The Security Officer shall document procedures for marking temporary materials that contain confidential/electronic P1-Il when created and establish a date for either destroying or bringing the materials under control as record documents.

C. All employees shall not leave any media containing confidential/electronic PHI unattended and/or open to compromise and indiscriminate copying.

RANKIN COUNTY HOSPITAL DISTRICT	
DEVICE AND MEDIA CONTROL POLICY	
# of Pages: 1 of 2	

II. ACCOUNTABILITY

A. The Security Officer shall maintain an inventory of all hardware and software in the organization as well as hard copies containing electronic PHI.

B. The Security Officer shall be responsible for the ordering, receiving, distributing, installing, and disposing of hardware and software.

C. The Security Officer shall maintain a record of the movements of hardware and electronic media and any person responsible for that movement.

D. The Security Officer shall keep the hardware and software inventory in a secure place.

E. The Security Officer shall have restrictions on who can view hardware and software inventory.

IV. DATA BACKUP AND STORAGE

A. The Security Officer shall have procedures to create a retrievable, exact copy of any electronic protected/confidential information, when needed, before the movement of equipment.

B. The Security Officer shall document procedures for backing up all electronic PHI data.

C. The Security Officer shall document procedures to always protect hard drives with electronic PHI.

D. The Security Officer shall document procedures to always protect tapes with electronic PHI.

E. The Security Officer shall document procedures to always protect diskettes, CD-ROMS or any other media containing electronic PHI.

RANKIN COUNTY HOSPITAL DISTRICT	
RCHD COMPANY VEHICLE POLICY	
# of Pages: 1 of 1	

RCHD Employees assigned to driving duties ("drivers") must at all times meet the following criteria:

- drivers must have a current, valid driver's license for the state in which the employee performs his or her driving duties; and
- drivers must maintain a clean driving record, i.e., must remain insurable under our company's liability insurance policy.

Any employee driving a RCHD vehicle or driving on RCHD business must observe all safety, traffic, and criminal laws of this state. No driver may consume alcohol or illegal drugs while driving a RCHD vehicle, while on RCHD business, while in a RCHD vehicle, or prior to the employee's shift if such consumption would result in a detectable amount of alcohol or illegal drugs being present in the employee's system while on duty. In addition, no driver may consume or use any substance, regardless of legality or prescription status, if by so doing, the driver's ability to safely operate a motor vehicle and carry out other work-related duties would be impaired or diminished. No driver may pick up or transport non-employees while in a RCHD vehicle or on RCHD business, unless there is a work-related need to do so. Any illegal, dangerous, or other conduct while driving that would tend to place the lives or property of others at risk is prohibited.

Anything a driver does in connection with the operation of motor vehicles can affect that driver's fitness for duty or insurability as a driver. Regardless of fault, circumstance, on- or off-duty status, time, or place, any driver who receives a traffic citation from or is arrested by a law enforcement officer, or who is involved in any kind of accident while driving, must inform an appropriate supervisor about the incident immediately or as soon as possible thereafter. Any penalty, fine, imprisonment, fee, or other adverse action imposed by a court in connection with such an incident must be reported immediately to an appropriate supervisor. In both of the above situations, the matter will be reported to RCHD's insurance carrier so that a prompt decision on continued coverage of the employee can be made. The driver involved in an accident or cited by a law enforcement official for violating a motor vehicle law must turn over any documentation relating to such incident as soon as possible to the employer, and must cooperate fully with the employer in verifying the information with other parties involved and with law enforcement authorities. While parking tickets will not affect a driver's insurability, any parking ticket issued on a vehicle that is being used for company business should be reported to an appropriate supervisor at the earliest possible opportunity.

Any employee who is involved in any traffic accident will be subject to a drug screen/alcohol screen. Any employee who violates any part of this policy, or who becomes uninsurable as a driver, will be subject to reassignment and/or disciplinary action, up to and possibly including termination from employment. All employees with driving duties must sign the following agreement:

I have read and understand the RCHD Driver Policy, and I agree, in the event that I am ever found to be uninsurable, or that I lack a clean driving record or a valid and current driver's license, that if necessary, I will accept whatever alternative assignment that RCHD may give me and that I understand that a reduction in pay, change in hours, change in duties, and/or change in work location may result from the reassignment. I further understand that RCHD does not and cannot guarantee that any particular reassignment will be available in the event of a problem with my driver's license, driving record, or insurability as a driver, and that if no reassignment is possible, termination of my employment may occur.

_____
Employee

_____
Date

RANKIN COUNTY HOSPITAL DISTRICT	
INTERNET/EMAIL POLICY	
1 of 1	

PURPOSE

Rankin County Hospital District maintains an internet connection and e-mail system that is available to designated employees performing as agents of Hospital business which includes:

Accessing, researching, and educational materials.
Communicating with other employees, peers, colleagues and outside agencies on business matters.

STANDARDS

Prohibited use - the Hospital District's internet connection or e-mail system may not be used for:

Copying or transferring copyrighted material without authorization from Administration.

Illegal Purposes

Personal communications or personal business

Political lobbying

Vandalism

Transmitting or receiving threatening, obscene or harassing materials

Facility Identification - The District is identified in every e-mail communication by the e-mail address. Any person in the public or private sector, including the medical sector may intercept these communications.

Privacy - Internal and external e-mail should not be used for communications that need to remain private or privileged under law or the provisions of Hospital District Personnel Policies.

Rules and Restrictions of the networks with which they connect and should communicate in a courteous manner.

Public Information - Any document published using the Hospital District's internet connection or e-mail system is considered an official record and is public information. Unless they are otherwise deemed confidential by law, these documents are subject to the Public Information Act.

RANKIN COUNTY HOSPITAL DISTRICT	
PASSWORD PROTECTION POLICY	
1 of 3	

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

This policy applies to all Rankin County Hospital employees that utilize Information Systems with IDs and passwords (credentials). This policy applies whether Staff is using RCHD Information Systems, Staff owned devices used for Company approved work, or Staff use Information Systems of third party service providers for work related activities.

Policy

The Security Officer shall ensure:

- Policies and procedures manage the process of creating, changing, and safeguarding passwords.
- Policies and procedures prevent staff from sharing passwords with others.
- Procedures advise staff to commit their passwords to memory and not allow them to be written down.
- Policies and procedures govern the password change frequency.

General

Passwords must be changed on a regular basis according to the following schedule:

- All system-level passwords (e.g., admin, root) must be changed every 30 days.
- All user-level passwords (e.g. e-mail, Web, desktop computer, etc.) must be changed at minimum every 90 days.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Passwords must not be inserted into e-mail messages or other forms of electronic communication. Passwords must not be stored or transmitted in clear (unencrypted) text.

Users are not permitted to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. Passwords/phrases shall be set for first time use and upon reset to a unique value for each user, and changed immediately by the user after the first use.

All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

Passwords are used to restrict access to systems, software applications, and data. Some of the more common uses of passwords include user-level accounts, Web accounts, e-mail accounts, screen saver protection, voice mail passwords, and device passwords (e.g. firewalls, routers, Smartphones, Wearable Computing Devices).

When selecting a password, Staff should remember that the longer and stronger the password, the more likely it will help keep Information Systems, and the data contained with the systems, secure.

Where possible, RCHD recommends that the passwords:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Include both numbers and special characters (e.g. @, #, $, *).
- Have a minimum of at least 10 characters and preferably fifteen alphanumeric characters long and is a passphrase.
- Don't contain personal information such as a relative or pet's name, social security or driver's license number, street address or phone number, etc.
- Avoid sequences or repeated characters. For example, 1234, 3333, etc.
- Not be common words such as those found in a dictionary.

Password Protection Standards

Do not use the same password for RCHD accounts as for other non-RCHD (e.g., personal e-mail, on-line banking, and social media).

Where possible, do not use the same password for various RCHD access needs. For example, select one password for e-mail systems and a separate password for access to systems that store sensitive or confidential data.

Do not share RCHD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential RCHD information.

Please remember:

- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not reveal a password to the boss.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.

RANKIN COUNTY HOSPITAL DISTRICT	
AUDIT CONTROLS POLICY	
# of Pages: 1 of 1	

POLICY

Rankin County Hospital District shall maintain logs of system activity. These system activity logs are required in order to recreate pertinent system events (including physical activities) and actions taken by system users and administrators. The audit process of examining logged information is required in order to identify questionable data access activities, investigate breaches, access the security program, and aid in responding to potential weaknesses.

PROCEDURES

A. The Security Officer shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected/confidential information.

B. The Security Officer shall implement and maintain audit logs to record access activity of electronic protected health information.

C. The Security Officer shall implement audit controls to examine access, including physical activity of electronic protected health information.

D. The Security Officer shall use audit control measures that are integrated with in the EHR software that helps track users who access patient information.

RANKIN COUNTY HOSPITAL DISTRICT	
IDENTIFICATION BADGE POLICY	
1 of 1	

PURPOSE

To specify requirements for employee identification through the use of identification badges.

POLICY

All employees will be issued and must wear identification badges as provided by the hospital. Identification badges must be worn in a manner that allows identification of an employee by photographic image, first and last names, and position title to be conspicuous to others.

DEFENITIONS

A. Identification Badges: a facility issued card containing identification information to be worn in a manner that clearly indicates the employee's name, job title, and other pertinent information to others.

RESPONSIBILITIES

Members of Administration and Department Supervisors are to ensure all employees wear identification badges while on duty.

PROCEDURE

A. The Human Resources Department will issue identification badges to all new employees
B. Identification badges will include the following information:
    a. Employee Picture
    b. Employee First and Last Name
    c. Employee Credentials, if applicable (eg. M.D, Ph.D, R.N)
C. Badges will be updated to reflect current information such as name or position changes.
D. Badges may be reissued once annually. If needed more frequently due to loss, the employee will be charged a $5.00 fee. There is no fee for issuing an identification badge when an employee's name changes or job title changes.
E. Badges must be clipped in the front of the person, at least six inches above the waist. Every effort should be made to ensure identification information is clearly visible to others. Badges must not be deliberately worn in a manner that prevents a person's name or job title from being visible.
F. Upon termination, the I.D. badge is to returned to the Personnel Office.

RANKIN COUNTY HOSPITAL DISTRICT	
INFORMATION SECURITY POLICY	
1 of 1	

POLICY

It is the policy of **Rankin County Hospital District** to evaluate technical and non-technical information security implementations in response to environmental or operational changes affecting the security if electronic protected health information.

PROCEDURES

DATA BACK-UP PLAN POLICY & PROCEDURE STANDARDS

A. **Rankin County Hospital District's** Security Officer shall perform periodic technical and non-technical evaluations in response to environmental or operational changes affecting the security of protected information.

B. **Rankin County Hospital District** shall have a designated internal audit group that performs technical evaluations of both information systems and network design for compliance with security standards.

C. **Rankin County Hospital District's** Security Officer shall maintain a technical evaluation history for both information systems and networks.

D. **Rankin County Hospital District** shall require that both information systems and networks be revised by the Security Officer if any additions or significant modifications are made to the design of the network.

E. **Rankin Counts hospital District** shall document all steps taken to ensure and maintain security compliance

RANKIN COUNTY HOSPITAL DISTRICT	
WORKSTATION SECURITY POLICY	
# of Pages: 1 of 4	

POLICY

Employees are responsible for maintaining the physical security of **Rankin County Hospital District's** computer resources under their control and for protecting the integrity and privacy of the data maintained on them by the appropriate use of lockdown devices, password controlled access, data encryption, virus protection software, and routine backup procedures.

Rankin County Hospital District reserves the right to inspect all data and to monitor the use of all its computer systems, and as such, workstation users have no right of privacy with regard to information on workstations. **Rankin County Hospital District's** right of access to personally owned computing devices will be limited to **Rankin County Hospital District's** patient or business information and applications important to maintaining security over that information, including, but not limited to anti-virus software, operating systems, etc. **Rankin County Hospital District** reserves the right to remotely access, monitor, control, configure workstations and any software residing on them.

Non-compliance with this policy is subject to management review and action up to and including termination of employment, vendor contract and/or legal action.

All workstations with fixed storage that support more than one user, and or process information including modems, must be equipped with security that secures hardware, and will or restricts access to software.

All workstations must be equipped with updated software for detecting the presence of malicious software (computer \ anti-virus). All computer and devices must have current version of anti-virus installed and operating at all times.

All workstations must be positioned or located in a manner that will minimize the exposure of any displayed patient or sensitive business information. When necessary, privacy screens should be deployed.

Users accessing the **Rankin County Hospital District's** network or information from remote locations, such as connections from home, should employ appropriate security safeguards.

The Security Officer shall have sole discretion in determining which hardware, operating systems, and connectivity solutions will be supported. Users may not, independently install connectivity hardware or software to the computing resources of **Rankin County Hospital District.**

All employees must comply with **Rankin County Hospital District's** policies, state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

POLICY & PROCEDURE STANDARDS

A. General

i. Users are required to log-off of applications containing patient health or sensitive business information before leaving their workstations.

ii. It is the user's option to save work on their hard drive (c-drive) or to the network. When the user does not use the network to store information and instead, uses other media, e.g. hard drive, diskettes, zip disks, etc, it is the responsibility of the user to make back-up copies of such information on a frequent basis

iii. In the event a critical document or file is inadvertently deleted, contact the IT Department immediately. *Do not continue to use the workstation,* or save additional work.

iv. All laptops and any other portable computer equipment must be secured (protected) when not in use. Proper security is dependent on risk factors and available resources at specific locations throughout the **Rankin County Hospital District.** Security may be provided by locking the equipment in a cabinet, desk, office, etc. Where such alternatives are not feasible, keeping the device out of sight in a desk or brief case may be appropriate.

v. Keeping information stored on a Portable Computing Device secure and current is the responsibility of the person who has the device in his or her possession and control. Those in possession are responsible for breaches of security related to devices in their possession.

vi. Password Protection: Workstations which are used to access patient health information or sensitive information are required to have password-protected capabilities for all users who are accessing patient information. Access to the EHR is specific in nature by user/function of user to enable a layered level of security when accessing patient records.

Department level procedures should define the allowable delay before automatic screensavers activate. That delay should be based upon a balance between operational needs and security risks. For example, consideration should be given to the:

- number of users having access to the application,
- number of patient records (high numbers are higher risk),
- location (higher traffic or public would be high risk)
- level of sensitivity of the information

vii. All systems containing sensitive patient or business information should enable auto log- off capabilities if available. The delay should be determined based upon the risk criteria above.

viii. Employees, physicians, volunteers, and outside vendors are required to have appropriate clearance prior to access to computer workstations.

ix. Upon termination or change of job position, users will have network access removed or modified.

x. Where possible, workstations should be segregated based on function and access privileges as it pertains to patient health or sensitive business information.

xi. All computing devices owned by **Rankin County Hospital District** shall be tagged and tracked by the Information Systems Department.

B. Workstations

i. **Rankin County Hospital District** has established standard configurations for desktop technologies deployed throughout the organization. All computers, computer peripherals and software as well as printers, faxes, and other miscellaneous hardware purchased with **Rankin County Hospital District** funds or attached to any component of the **Rankin County Hospital District's** network must meet these standards.

ii. Installation of personal software, purchased or downloaded, including, but not limited to screensavers and animated GIFs, by employees is prohibited. Software required for end user purposes must be approved and installed by the Information Systems Department. The end user must document and maintain proof of license to have such applications. Software installations will be coordinated through Information Services.

iii. Workstations must be installed with physical safeguards to eliminate or minimize the possibility of unauthorized access to information or theft of equipment. To the extent possible, equipment should be located in areas that have some degree of physical separation from the public and, where possible should face away from the public. In instances where the workstation cannot be kept out from public view, privacy screens are mandated

iv. Computer access and password training, provided by the Information System Department, must be completed before access privileges are granted to ensure adequate training has occurred.

v. **C. Portable Computing Devices**

i. The loss or theft of any portable computing device on which a **Rankin County Hospital District's** patient or sensitive business information is stored shall be immediately reported to the Security Officer whether or not the hardware is owned by the **Rankin County Hospital District.**

ii. Start-up authentication and authorization passwords (user name and password) are required on all portable-computing devices that store patient health information (PHI) or confidential data whether or not the hardware is owned by **Rankin County Hospital District.** Additional passwords and/or encryption may be required at the discretion of the Information Systems Department.

iii. Passwords and user IDs for computer systems and networks must not be stored on portable computing devices.

v. Portable computing devices that have stored data belonging to **Rankin County Hospital District,** may not be shared with others who are not authorized to access that information unless that information is stored as encrypted password protected files.

vi. The installation of virus protection programs is the responsibility of the user, except where a **Rankin County Hospital District** device is connected to the **Rankin County Hospital District** network, which will install and run appropriate antivirus protection.

vii. Vendors, consultants, business associates and all others wishing to connect portable computing devices to the **Rankin County Hospital District** network must first submit the equipment to **Rankin County Hospital District** Information Services for inspection of the adequacy of anti-virus software and installation of critical operation updates.

Remote Access

Access to **Rankin County Hospital District** internal network from outside of its defined network perimeter must be controlled by privileged access controls that may only be established by the Information Systems Department. Users are not authorized to install connections such as modems. PC Anywhere. etc. Dial-in access and Virtual Private Network (VPN) connections should be strictly controlled using one time password authentication.

It is the responsibility of users with dial-in access and VPN privileges to ensure that a dial-in connection to **Rankin County Hospital District** is not used by non-authorized individuals to gain access to company information or to internal networks. Users with remote access from personally owned computing devices have responsibility to employ security protections that can prevent their computing device from passing along viruses or similar internet threats to the **Rankin County Hospital District** network and data.

RANKIN COUNTY HOSPITAL DISTRICT	
KEY CONTROL POLICY	
# of Pages: 1 of 2	

PURPOSE

The purpose of this Key Control Policy is to establish reasonable personal security for members of the Rankin County Hospital District and to ensure the protection of property through the control of keys to resident rooms and other secure areas. The responsibility for implementing this Key Control Policy is with the Administration of Rankin County Hospital District.

KEY ISSUANCE

All keys are the property of Rankin County Hospital District and will be issued through the Maintenance Department or its designees.

Key requests must be submitted to the Department Head and be approved by the CEO.

A key holder's privileges can be revoked at any time by the Department head or an appropriate administrator.

KEY HOLDER RESPONSIBILITIES

Individuals issued a key are responsible to safeguard the key and maintain security of Rankin County Hospital District or area which the key opens. By accepting a key an individual agrees to:

1. Protect the key from theft or loss.
2. Not duplicate, loan or allow any other individual to use the key.
3. Use the key for Rankin County Hospital District business only.
4. Assure that doors are relocked after entering or leaving.
5. Report to the RCHD Maintenance Department any condition which may jeopardize people or property.
6. Assume responsibility for the conduct of any person the key holder allows to enter a locked facility.
7. Immediately notify the RCHD Maintenance Department when any key is lost or stolen.

RANKIN COUNTY HOSPITAL DISTRICT	
KEY CONTROL POLICY	
# of Pages: 2 of 2	

Lost/Stolen Keys

Lost or stolen keys must be reported to the RCHD Maintenance Department by the quickest means available. An incident report will be completed and a copy of the report will be forwarded to the Administrator.

When a key is lost, the locks will be modified to render the current key inoperative. The lock core/cylinder will be replaced in the existing lock and the new key will be issued to the owner. Exceptions are only on approval of the CEO/Administrator.

The fee for a replacement key will be $100.00. The fee will include the cost of the replacement core, key and actual labor charges. A record will be kept of all individuals who have replacement keys. Any subsequent loss of a key will result in a replacement fee of $150.00. The individual will be considered for disciplinary action on the third loss of a key. Subsequent losses will subject the individual to further disciplinary action.

Duplication of Keys

No key will be duplicated except by approval and control of the RCHD Maintenance Department. The unauthorized duplication of RCHD keys so adversely affects the security of persons and property that violations of this rule are considered serious and grounds for termination.

As an Employee of Rankin County Hospital District, I agree and will comply with all the rules and regulations as stated in the policy above.

_____ _____

PRINTED NAME SIGNATURE

DATE _____

Policy/Procedure No:
Approved By:

POLICY AND PROCEDURE MANUAL

Fire Safety Policy & Plan

For
Rankin County Hospital District
Issued by the Safety Department: Reviewed/Revised: 07/31/2015
Reviewed & Approved by the Safety Committee:

PURPOSE: The purpose of the Fire Safety Policy and the use of "CODE RED" is to safeguard patients, personnel and hospital property by a thorough understanding and practice of fire control procedures and emergency evacuation of patients.

Fire Safety is the responsibility of all hospital employees. The responsibility of a department manager is to implement the procedure devised by the Administration in the event of fire. Each employee must know the fire plan and their individual role.

POLICY: Rankin County Hospital District is monitored by an electronic fire detection and alarm system. The main control panel and annunciation is located at the nurses station with an instruction sheet attached to the wall just below the annunciation panel. A copy of the instruction sheet is listed as APPENDIX 1 of this policy.

There are audible and visual alarms maintained in all areas of the hospital. The hospital also has clearly marked and readily accessible fire extinguishers placed in various places throughout the hospital.

PERSONNEL INVOLVED:

All hospital personnel shall be involved in the fire safety program.

A. FIRE PREVENTION:

1. Housekeeping & Maintenance is the first step in fire prevention. The Housekeeping & Maintenance Departments will ensure that there is no reasonable potential for the ignition of a fire by maintaining a clean safe working environment of the facilities.
2. All hospital staff will keep a watch for any questionable fire hazard. Any possible hazard will be reported to the maintenance/safety office. The Maintenance Director will then take the appropriate steps to correct the problem or incident.
3. Watch for signs of fire. Night hours are a higher risk period for the spread of a fire since hospital traffic is at its minimum.
4. All hospital staff is expected to keep and maintain their work areas in a safe healthy work condition.
5. Keep all areas clean and free from non-essential materials and equipment.
6. Assure that an electrician or bio-medical engineer checks all electrical equipment regularly.
7. Enforce "NO SMOKING" regulations inside all hospital facilities. Smoking is prohibited inside of all hospital facilities and within 10 foot of the medical gas cages. Smoking is allowed outside of the buildings, in the central break area, and at least 10 foot away from gas cages.
8. All staff shall know the location of fire extinguishers, alarm pull stations and how to operate them.
9. All staff shall know the locations of the building exits.
10. All staff will know and regularly review the hospital's plans for fire control and evacuation.

B. FIRE EVENTS:

A "fire event" is any event in which the fire detection equipment makes a call. All "fire events" will result in the monitoring service making a call to the Law Enforcement & Fire departments, Service Company, Hospital Administration, Maintenance Director. A fire event can include one or more of the following:

1. Fire Drill: An unannounced, staged practice event.
   a. A fire drill will be treated as if an actual fire was in effect.
   b. All "Code Red" procedures will be followed.
   c. An evaluation report will be written and filed upon all fire events.

2. False Alarm: An unintentional call for the fire detection system to sound an alarm.
   However, all false alarms will be treated as a "CODE RED".
   "CODE RED" procedures will be outlined later in this policy.
   This includes but is not limited to the following:
   a. Food being overcooked in a microwave.
   b. Someone bringing a lit cigarette into the building.
   c. Dust getting into a smoke detector (Which may also be reported as a supervisory alarm.)

3. Supervisory Alarm: An electrical or mechanical interruption of a point in the fire detection equipment. A supervisory alarm may include but is not limited to:
   a. Malfunction of any point or piece of fire detection equipment.
   b. Someone is tampering with (with intent to damage) or manually operating the fire detection equipment.
      Any attempt to intentionally damage or sabotage the fire detection equipment will result in arrest and criminal charges being filed. If in the event an employee tampers with or sabotages the fire safety equipment it will result in employment termination, arrest and criminal charges being filed.
   c. Manual operation may be attempted during systems repair, inspections and/or maintenance.
   d. A supervisory alarm needs to be immediately reported to the maintenance/safety department.
   e. The Maintenance Director will inspect the problem and have repairs made to the system. A record of all supervisory alarms will be recorded and filed in the Fire Safety Log Book in the maintenance/safety office.

4. Fire: "CODE RED" An actual event of a fire in or on the hospital facility and/or grounds.
   a. Procedure will follow under section C.

C. "CODE RED":

Procedure: see also flow chart on Appendix 2

1. DO NOT use the word "FIRE!" at any time. This could cause panic.
   a. At the first sound of the alarms the Charge Nurse is to immediately examine the annunciation panel display. Silence the Alarm and use the displayed information to make the following announcement over the intercom. Three (3) times:
      "CODE RED in _____. All Personnel secure their areas, shut off all gas valves, make sure all doors are closed, acquire necessary equipment and assist in _____."
   b. Charge nurse is to head the fire safety operation until the arrival of the Fire Department at which time the charge nurse will defer all safety operations to the present Fire Captain.
   c. Charge nurse is to notify the Maintenance Director by phone as soon as possible if he is not already present.

d. Charge nurse is to see that all personnel are in assigned locations and performing their assigned duties.

2. Personnel at Fires Point of Origin
   a. If the fire is in your area, Keep Calm and do not panic.
   b. Report the fire by pulling the nearest fire alarm pull station. If the fire detection equipment has not already done so. The Fire department will be notified automatically.
   c. Move all patients out of the danger area.
   d. Close all doors and windows; turn on all lights.
   e. Report to the charge nurse and notify the exact location of the fire and if possible what is burning and where.
   f. Shut off oxygen, nitrogen and vacuum valves in fire area(s).
   g. Attempt to extinguish the fire using the proper equipment if you can safely do so.
   h. Keep all communication systems open for emergency calls. If someone is using the phone at the time, the call is to be terminated immediately unless it is in the scope of emergency use. This includes landlines, cellular phones, and radios (both receivers and transceivers).
   i. In case of smoke, use wet linen or blankets at the bottom of the doors. Remember smoke always rises. Therefore, if necessary, get patients and visitors to lie down on the floor.
   j. For an evacuation, use wheelchairs, stretchers, beds, blankets, etc.
   k. Get visitors to evacuate hospital. Man the exterior doors to prevent visitors from reentering building.
   l. If you're assigned or ordered to monitor a station remain there unless otherwise notified. Always stay calm.

3. Personnel Away from Fire's Point of Origin
   a. Acquire fire extinguisher and report to location of fire as announced over the intercom by the charge nurse, unless ordered to do otherwise by the charge nurse or fire department personnel.
   b. Man any exterior door in your area to prevent visitor(s) from entering building.

4. All personnel not directly involved in fighting the fire will do the following:
   a. Close all open doors.
   b. Retrieve any ambulatory patients and visitors from corridors.
   c. Reassure patients.
   d. Remain with the very ill, elderly or pediatric patients.
   e. Anticipate evacuation of hospital.
   f. Ensure all hospital exits are closed and do not allow visitors to enter the facility. A staff member shall man each exit to ensure compliance.
   g. Help in the evacuation of all visitors in the hospital lobby and halls. Evacuation of all visitors is mandatory.

5. All physicians should be ready for evacuation of patients.

6. Authorization to cancel "CODE RED" and reset fire alarm system
   a. The fire alarm system is not to be reset until all areas are searched and the fire is extinguished or the cause of the alarm has been determined by Fire Department personnel and/or safety officer as all clear.
   b. Afterward the safety officer, Administrator, or charge nurse will authorize All Clear.

7. Authorization to evacuate patients and Personnel
   a. The command to evacuate the hospital will be given by the charge nurse, Administrator or designee, or a Fire Department representative.

D. EVACUATION INSTRUCTIONS

All hospital visitors in the halls and lobby will be required to evacuate the hospital during all fire events.

1. Partial Evacuations
   a. If partial evacuation is determined, patients will be moved to a safer part of the building.

2. General Evacuations
   a. If a general evacuation is determined, all hospital occupants will be evacuated to a location outside of the building. All patients being evacuated to the outside of the Hospital should be protected from exposure to weather as much as possible.

3. Evacuate patients according to their physical condition. The charge nurse will ensure all patients are accounted for.
   a. Ambulatory Patients: these patients should be led in a group to a safe area.
   b. Wheelchair Patients: These patients will be evacuated by wheel chair so that other patients can be evacuated.
   c. Stretcher Patients: Those nearest to the danger areas will be evacuated to a safe area first. Patients will yield stretchers after reaching safety if there is need. Sheets and blankets may be used to slide patients along the floor to safety.
   d. Infants and children: These are the most helpless of all patients. At the first sign of danger, remove them to a safe area. Infants and small children may be placed in their parent's/guardian's care after being moved to the safe area.

4. During the evacuation use caution and common sense. Be prepared beforehand:
   a. Always touch a closed door with the back of your hand before opening it.
      IF IT IS HOT DO NOT OPEN IT.
      DO NOT TOUCH THE METAL DOOR HANDLE. If a fire is on the other side of the door the door will be hot and the metal handle could transmit enough heat to cause severe burns.
   b. Tag each room to indicate that the room is "Completely Evacuated" with a piece of tape on the outside door or door handle.
   c. Each patient should have a blanket from his bed placed around his shoulders before being evacuated.
   d. Learn and practice several transfer techniques for evacuating patients.
   e. Always move patients toward the closest available exit.

E. FALSE ALARM:

Procedure:

1. DO NOT use the word "FIRE!" at any time. This could cause panic.

2. Until the charge nurse is notified that there is a false alarm the procedure of "CODE RED" will be followed.
   a. At the first sound of the alarms the Charge Nurse is to immediately examine the annunciation panel display. And use the displayed information to make the following announcement over the intercom. Three (3) times:
      "CODE RED in _____. All Personnel secure their areas, shut off all gas valves, make sure all doors are closed, acquire necessary equipment and assist in _____."
   b. In the event that personnel report to the charge nurse that there is a false alarm and explain the problem. The charge nurse is to announce the following over the intercom.
      "CODE RED – All CLEAR, CODE RED – ALL CLEAR, CODE RED – ALL CLEAR "
   c. Charge nurse is to call the fire department (693-2252) and law enforcement offices (693-2422) and report that there is a false alarm and to cancel mobilizing emergency services. Also the monitoring service should be informed of the false alarm (866-491-3400) pin# 114615.

d. Charge nurse is to notify the safety officer by phone as soon as possible if he is not already present and report the incident to him.
e. Maintenance Director (or his appointee) is to write up a report of the incident for documentation and have the charge nurse and the personnel that reported the false alarm to sign the documentation and file it in the Fire Safety Log Book located in the Maintenance/Safety Office.

E. FIRE KNOWLEDGE:

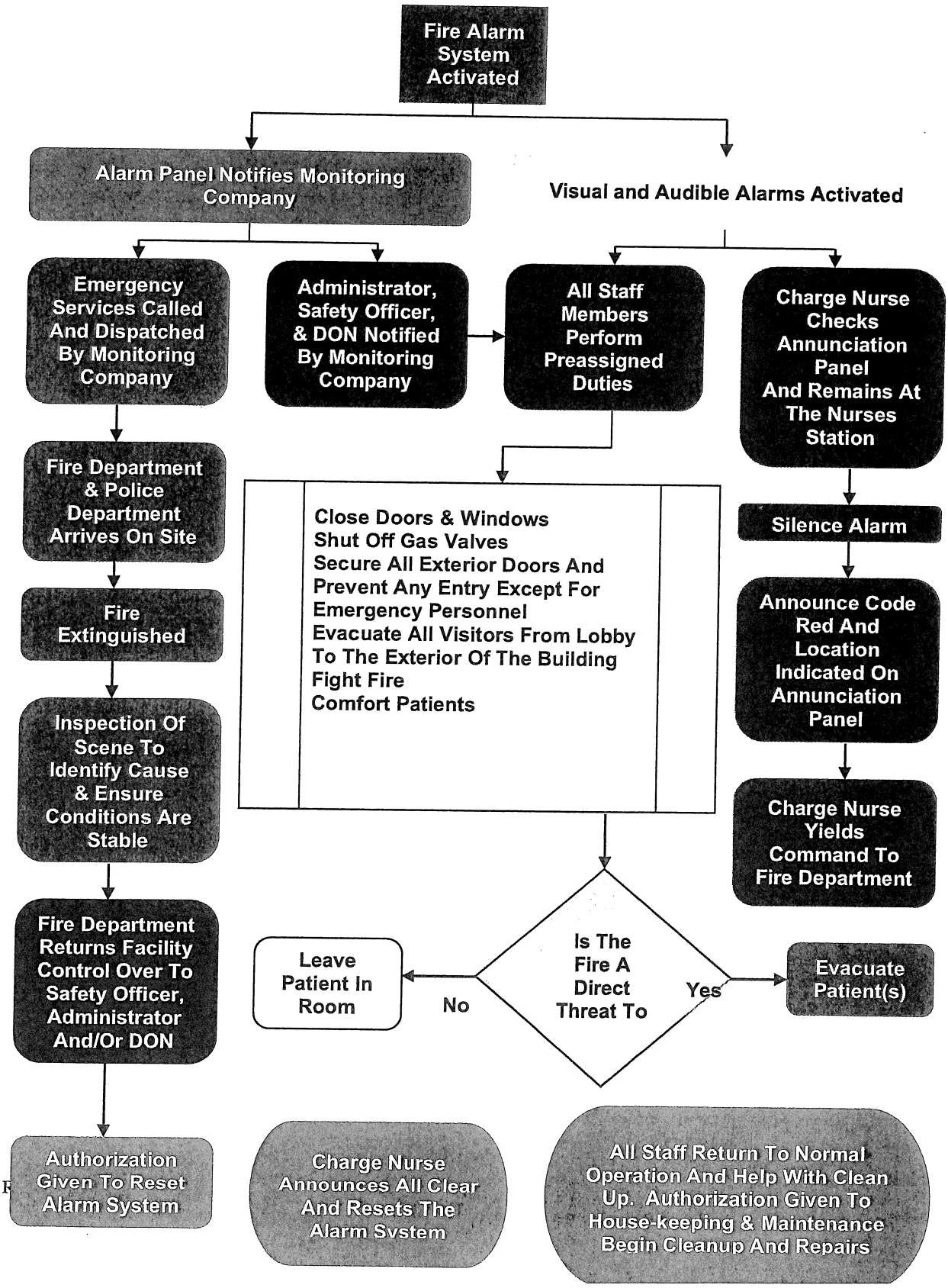
1. Each Department Manager in cooperation with the Maintenance Director/ Safety Officer shall instruct all employees in the operation of the fire safety program and of their duties. Each employee shall be familiar with the fire alarm system and how to activate it.
2. Department Managers are responsible to instruct the personnel as to the Fire Safety Policy & Plan.
3. The Maintenance & Safety Director will decide on the date, time, location and nature of fire drills. A fire drill report shall be filed on each drill with the signatures of all participating personnel. This fire drill report will critique the actions of personnel and make observations and recommendations to be discussed at the next hospital staff directors meeting. This fire drill report shall be filed in the Fire Safety Log Book located in the maintenance/safety office.
4. Fire drills will not be pre-announced to hospital personnel.
5. There are three classes of fires;
   a. CLASS A: Combustible (paper, wood, cloth, etc.)
      Use pressurized water extinguisher or water or ABC extinguisher.
   b. CLASS B: Flammable Liquids (gasoline, oil, fats, alcohol, etc.)
      DO NOT USE WATER!
      Use CO2 extinguisher, Baking Soda, Dry chemical, or ABC extinguisher.
   c. CLASS C: Electrical Equipment (appliances, wiring, etc.)
      DO NOT USE WATER!
      Use dry chemical, CO2 or ABC extinguisher.

NOTE: AN ABC EXTINGUISHER MAY BE USED ON ALL FIRES

APPENDIX 1

Fire safety system operating instructions of currently installed fire equipment.

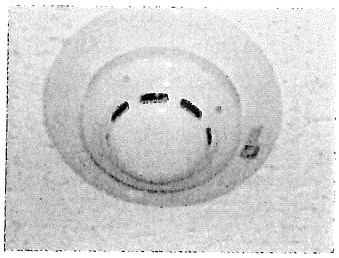
APPENDIX 2
Sequence Of Operation



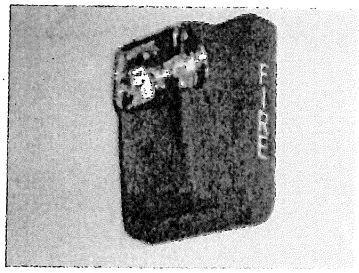
APPENDIX 3
Identification of Points

The current Fire Safety is set up with points or locations.
The following are photos identifying the various point or location types of Fire Safety equipment installed in the Hospital:

Pull Stations



Smoke Detectors



Visual & Audible Alarm Indicator

Fire Extinguisher

Fire safety Policy & Plan for Rankin County Hospital District was reviewed/revised by the Safety Department on 10/01/10; it was reviewed and authorized by the Safety Committee on 10/07/2010

Code Red Procedure

Step 1.When the Fire Alarm sounds check the annunciation panel

Step 2.Press the down arrow on the annunciation panel and find the origin of the alarm.

Step 3.Insert the black plastic alarm panel key and turn it and press the "Silence" button (once only) on the annunciation panel. Leave the key in this position.

Step 4. Make the following announcement over the intercom.

"Code Red in (location). All personnel secure their areas, make sure all doors are closed, acquire necessary equipment and assist in (location)."

Step 5. Charge nurse is to call emergency services (police and fire departments # 693-2422) to inform them of the situation.
(Exception: Safety Officer informs the charge nurse that "This Is A Drill.")

Step 6. Charge Nurse is to contact the Maintenance / Safety Officer if he is not present.

Step 7. Charge nurse is to remain at the nurse's station. All other personnel are to follow the procedures as announced over the intercom.

Step 8. After approval from the Safety Officer, or Administrator, or Fire Department personnel the charge nurse is to announce the following.

"Code Red All Clear, Code Red All Clear, Code Red All Clear"

Step 9. After approval the Safety Officer or Charge nurse is to press the "Reset" button (once only) and then turn the black plastic alarm panel key and remove it to reset the system.

Step 10.Reassure and comfort all patients.