

# **FAITH REGIONAL HEALTH SERVICES POLICY AND PROCEDURE**

## **HIPAA: Data Contingency Plan**

PAGE 1 OF 3

### **I. PURPOSE:**

It is the policy of Faith Regional Health Services to secure electronic data from damage or loss.

### **II. SCOPE:**

This policy applies to all employees of Faith Regional Health Services.

### **III. PROCEDURE**

#### **Plans to respond to a system emergency:**

#### 1. Applications Criticality Analysis:

- Policy:
  - All computer software applications are analyzed to ensure the integrity of the stored information.
  - Every computer software application is assessed monthly for the integrity of firewalls, pass codes, passwords, storage capacity, and transmission capabilities.
  - Documentation of the monthly assessments are maintained by the Privacy Officer.

#### 2. Data Backup plan:

- Policy:
    - Protection of computer data is performed through a back-up for stored information.
    - Entire system is copied onto magnetic tapes each evening as part of the nightly system shutdown procedure. There are no exceptions to this process.
    - Nightly back-up tapes are rotated on a daily basis, 7 days per week, 365 days per year.
    - All back-up tapes are stored off-site in a fire resistant enclosed container located at
- 

#### 3. Disaster Recovery Plan:

- Policy:
  - There is a plan to maximize the confidentiality of information and to maintain operations in the event of a disaster to include fire, vandalism, natural or system failure.
  - **Fire:** In the event of a fire, the following is to be done:
    - Ensure that no employee is in immediate danger.
    - Close the doors around the fire area.

- Sound the alarm by pulling the fire alarm and notifying the operator by dialing '6111' and giving the physical location of the fire.
- Unplug all electrical equipment
- Secure all confidential records inside a fire-resistant storage cabinet.
- Remove as much portable equipment as possible.
- Maintain personal safety
- Await confirmation from Fire Department personnel before returning to the fire location and resuming operations.
- **Vandalism:** In the event of vandalism, the following is to be done:
  - Request that nothing be touched in the area affected by vandalism.
  - Notify security immediately
  - Secure the site of the vandalism
  - Provide inventory of information, data, and equipment that was vandalized.
  - Await confirmation from Security Personnel before resuming operations.
- **Natural Disaster:** In the event of a natural disaster, the following is to be done:
  - Ensure safety of all personnel
  - Secure the region by closing all available doors or erecting barriers around the area.
  - Conduct an inventory of information, data, and equipment that was damaged.
  - Identify needs for replacement of information, data, and equipment.
  - If necessary, obtain back-up tapes from off-site storage facility and input them into the system.
  - Utilize all available resources to resume and maintain operations.
- **System Failure:** In the event of a system failure, the following is to be done:
  - Establish the integrity of the Information Services Department
  - Determine the degree of information in the computer systems at the time of the system failure.
  - The Director of Information Systems will determine the amount of information loss, if any, from the failure.
  - The Director of Information services or designee will notify all effected departments of any information lost to allow for appropriate retrieval of information.
  - If the Information Services Department is intact:
    - Notify the Director of Information Systems or designee if the failure occurs during off-hours. This individual will in turn notify all other employees of effected departments of the system failure.
    - Employees are to revert to the use of manual patient information collection and documentation until the computer system failure has been resolved.
    - Manually collected patient information and documentation will be inputted into the electronic system immediately upon resolution of the system failure.
  - If the Information Services Department is not intact:
    - Notify the Director of Information Systems and hospital Administrator immediately.

- The Director of Information Systems will assess the situation immediately upon arrival and inform the hospital Administrator of the degree of damage.
  - The Director of Information Systems or designee will notify all other personnel of affected departments as soon as possible.
  - The Director of Information Services or designee will contact the facility's computer system Customer Service Department and report the situation.
  - Direction will be taken by the Customer Support Department.
  - Obtain back-up tapes from off-site storage facility to install in preparation to maintain operations.
  - Employees are to revert to the use of manual patient information collection and documentation until a contingency computer system has been installed.
  - Manually collected patient information and documentation will be inputted into the contingency system immediately upon resolution.
4. Emergency Mode Operations:
- Policy:
    - The emergency mode operations plan is implemented in the event of a fire, vandalism, natural disaster, or system failure.
    - Notify the Director of Information Systems of an emergency.
    - If possible, ensure the security of the electronic information by closing doors and restricting access except to personnel authorized by the Director of Information Services, the Privacy Officer, and the hospital Administrator.
    - Determine the effects of the emergency and implement the appropriate plan: fire, vandalism, natural disaster, system failure.
    - Maintain the selected emergency plan until the emergency is resolved or a contingency plan is implemented to maximize operations.
5. Testing and Revision Procedures:
- Policy:
    - System emergency plans and procedures are tested every two (2) months.
      - The Director of Information Systems creates a schedule to test each emergency plan and procedure
      - Each plan is tested in a controlled environment
      - The outcome of each test is documented and matched with the established plan and procedure.
      - Changes are made to the plans or procedures as identified from the testing.
      - Documentation of the testing is maintained by the Privacy Officer.