

**DRAFT**

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

## **HIPAA: Security Management Process**

PAGE 1 OF 2

### **I. PURPOSE:**

It is the policy of Faith Regional Health Services to manage the security of all confidential patient healthcare information.

Faith Regional Health Services believes that all patient healthcare information is confidential and must be kept in a secure manner. Faith Regional Health Services upholds the highest level of security for all confidential patient healthcare information. In the event of any breaches of this security, Faith Regional Health Services will strive to recover the information released in the breach, identify the employee(s) responsible for the breach and discipline those responsible for the breach.

### **II. SCOPE:**

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

### **III. PROCEDURE**

1. The Director of Information Systems is responsible for overseeing the integrity of the security management process.
2. The Security Management Process includes:
  - a. Roles and responsibilities of the Director of Information Systems to include overseeing the implementation of security policies, employee education regarding security measures, integrity of electronic communication, the physical security of the information and decisions regarding the abuse or misuse of the information.
  - b. The Director of Information Services in conjunction with the hospital Administrator has selected and implemented security processes that secure the confidentiality and integrity of confidential patient healthcare information in the most cost-effective manner.
  - c. The Director of Information Systems in conjunction with other hospital committees uphold the process to reduce breaches to confidential patient healthcare information.
  - d. Hospital employees are trained on the security measures regarding confidential healthcare information. This information is provided upon initial orientation to the hospital as a new employee and reviewed annually by the Trainer and the Information Services Department.
3. Hospital employees found breaching the confidentiality of patient healthcare information will be placed in the disciplinary process to include:

PAGE 2 OF 2

HIPAA/ Security Management Process P&P/kcwRevised 2/13/02

**First Offense:** Verbal warning; documentation of such will be placed in the employee's permanent record.

**Second Offense:** Written warning; documentation of such will be placed in the employee's permanent record.

**Third Offense:** Limited use of access code only upon supervision from the department manager; placed on probation for three (3) months; documentation of such will be placed in the employee's permanent record.

**Fourth/Final Offense:** Termination of employment; documentation of such will be placed in the employee's permanent record; notification to appropriate licensure boards of violation of confidential patient healthcare information (i.e., State Board of Nursing, AMA).

4. Business Associates/subcontractors of the hospital are expected to maintain the confidentiality of patient healthcare information. If found in violation of this confidentiality of patient healthcare information. If found in violation of this confidentiality, the following will occur:
  - a. Provide notice of civil or criminal penalties for misuse or misappropriation of healthcare information.
  - b. Violations may result in notification to law enforcement officials, regulatory agencies or accreditation agencies.
  - c. Limit use of system privileges or cease all use of system privileges.
  - d. Enforce violation of contract penalties.
5. The security management process is evaluated and reviewed annually by the appropriate hospital committees and hospital Administrator.
6. Documented changes to the security management process will be communicated to all employees on a routine basis.
7. The Information Systems Department is responsible for ensuring all employees have been notified of any changes to the Security Management Process to include the name of employee and date of training.