

Policy and Procedure Number:
Effective:

Protection/Access to Electronic Protected Health Information

Purpose

The Jackson County Health Department is committed to maintain the privacy of electronic protected health information. The health department administration will ensure that only those needing this information in order to perform the functions of their job position will be given access to electronic protected health information.

Policy

1. The Administrator and/or the Information Security Officer will be responsible for the assignment of user identification numbers for staff needing access to protected health information in order to perform the functions of their job position.
2. All computer programs containing electronic protected health information will be protected by requiring an assigned user identification and an employee designated password.
3. These passwords will be set to require changing at a minimum of once in a sixty-day period if not more frequently.
4. Employees will not share their user identification and password with anyone. If it is determined that this security breach has occurred, the employee releasing their password will be disciplined following the Department of Health and Human Resources Progressive Discipline Policy.
5. Upon termination or resignation of an employee, all access to protected health information will be terminated by the Administrator and/or the Information Security Officer.

Procedure

1. Upon employment, the Administrator and/or the Information Security Officer will determine whether the employee needs access to a protected health information database in order to perform their job.
2. The Administrator and/or the Information Security Officer will make the necessary arrangements for user identification number assignment.
3. The temporary password will be set requiring the employee to change the password upon entry into the system.
4. All programs containing protected health information will require the user to change their password on a regular basis; however, not in excess of sixty (60) days.
5. If an employee is locked out of their system or program, they will contact the Administrator and/or the Information Security Officer to reset their password.
6. Staff releasing their user identification number/password will be disciplined in accordance with the Department of Health and Human Resources Progressive Discipline Policy.