

Policy and Procedure Number:
Effective:

Facility Access/Security

Purpose

The Jackson County Health Department will ensure that physical access to its electronic information systems and its facilities is limited. Only those authorized will have access to the computer systems.

Policy

1. The front and rear doors of the main health department will be double locked when the facility is not in use. The front and rear doors of the satellite office will be locked when the facility is not in use.
2. All keys to the buildings will be numbered and engraved "do not duplicate."
3. Employees will be assigned a numbered key and must sign for the key. The employee will be instructed not to allow anyone access to their key without written permission from the Administrator or the Information Security Officer in the absence of the Administrator.
4. No individual will be allowed outside the reception area without being accompanied by an employee.
5. No individual will be left alone in a room containing protected health information.
6. All staff will log off their computer when leaving their office.
7. No individual will be given access to the computer/server without prior approval of the Administrator and/or Information Security Officer.
8. A Computer/Server Access Log will be maintained by the Administrator and/or Information Security Officer. This log will include the name, date, time, and purpose for every individual accessing the computer system.
9. Employees violating this policy will face disciplinary action as defined by the Department of Health and Human Resources Progressive Discipline Policy.
10. Administrator and/or the Information Security Officer will work with the Office of Management Information Systems to relocate the computer server and other equipment to a locked closet/cabinet.

Procedure

1. At the end of each business day, the front and back doors of both buildings will be locked.
2. All rooms containing protected health information or the computer server will be locked at the end of the day.
3. Upon employment, staff will be given and will sign for their access key. The employee will be instructed not to allow anyone access to their key without written permission from the Administrator or the Information Security Officer in the absence of the Administrator.
4. The back door of both buildings will remain locked during normal operating hours unless accessed by an employee with a key.

5. Individuals coming into the health department will be greeted in the reception area and will remain there until the appropriate staff member escorts that individual through the building.
6. No individual will be left in a room with access to protected health information.
7. Staff will log off of their computer when not in use or when they leave their office.
8. If a computer technician or anyone else requests access to the computer system or server, the Administrator and/or the Information Security Officer will be notified prior to access being given.
9. The Administrator and/or the Information Security Officer will maintain a Computer/Server Access Log documenting person, date, time and purpose of the event.
10. The Administrator and/or the Information Security Officer will ensure that the proper Business Associate Agreement and/or Confidentiality Statement are signed and in place.
11. Employees violating any portion of this policy will face disciplinary action in accordance with the Department of Health and Human Resources Progressive Discipline Policy.