

Policy and Procedure Number:
Effective:

Electronic Protected Health Information Storage and Inventory

Purpose

The Jackson County Health Department is committed to maintaining all individuals privacy in regards to their protected health data and the conduct of personnel in relationship to this data. The Jackson County Health Department staff will work to ensure that all health data be stored and tracked to maintain confidentiality of this data.

Policy

1. The policies and procedures stated herein apply to all electronically maintained or transmitted health information pertaining to an individual.
2. Employees shall log into health information systems using their privately assigned identification number and password. This information shall be keep confidential as per Board of Health adopted computer usage policies.
3. At the completion of a work session or departure from their desk, an employee shall log-off of programs accessing protected health information.
4. All protected health information must be maintained on the server located at the main health department building. No one is authorized to save protected health information on their hard drive at any time.
5. All protected health information saved to the server shall be backed-up according to Back-Up Performance and Storage Policy.
6. The inventory of electronic protected health information applications shall be updated as new software applications processing this data are added to the system.
7. Only staff working directly with the protected health information will be given access to that data.

Procedures

1. Employees must log-on to their computer with the provided identification and password. Upon completion of data entry or the employee leaving their desk, they must log-off of programs accessing protected health information.
2. Electronic health information will be maintained primary in three databases, one for Home Health, one for Immunizations, and one for all other public health data.
3. The assigned support personnel will replace the back-up weekly and notify the Security Officer and Management Information Systems (MIS) if the system is not working properly.
4. The inventory within this document will be updated periodically by the Security Officer. If new programs are added, they will be added to the server and the Security Officer will ensure that the system is secure and only those working with the data will have access to the data.