Cumberland County Hospital System, Inc.
Administrative Policy - Procedure

TITLE:	POLICY NUMBER	APPROVED BY	EFFECTIVE DATE	Page 1 of 2
CONFIDENTIALITY AND INFORMATION ACCESS POLICY		**MN**	**8/1/97**	

POLICY: Cape Fear Valley Health System (CFVHS) provides workforce members with data and information needed to carry out their duties quickly, efficiently, and effectively. In addition to workforce members, this policy applies to outside contractors, consultants, staff of affiliate organizations, or anyone given authorized access to any of CFVHS's information. Access to information is based upon the "need to know" principle. Reasonable access is defined as access broad enough to allow individuals to make legitimate use of information in carrying out CFVHS duties and, at the same time, restrictive enough to guard against inappropriate access.

PURPOSE: To safeguard the integrity and reasonable access of CFVHS data and information and to protect and safeguard confidential and proprietary information pertaining to patients, caregivers, employees and CFVHS operations.

DEFINITIONS:

Integrity of computer-based information systems is defined as having the ability to recover, audit, and verify the data on the system.

Workforce as defined in the Health Information Portability Accountability Act (HIPAA) Security and Privacy Regulations means employees, volunteers, trainees, and other persons who work within CFVHS, whether or not CFVHS pays them.

ACCESS: Users are to complete the Computer Access Form available on the InfoWeb. The Department Manager is to review and determine applications to which the workforce member needs access. The identified applications administrator is to work with the designated Information Services and Technology (IST) Coordinator, as needed, to determine if the access is warranted and justified prior to access being granted. Each outside contractor, consultant, or staff of affiliate organizations is to have a department management sponsor.

CONFIDENTIALITY AGREEMENT:

1. Prior to gaining access authorization and then annually, users who are granted computer system access are given a copy of this policy and are asked to sign the Information Access and Confidentiality Agreement (Agreement). It is the responsibility of the Department Manager to have the Agreement signed by staff and those whom they sponsor.
2. Physicians and Allied Health Practitioners are to sign the Agreement as part of the credentialing process and each time they are re-credentialed.

Reviewed/Revised	Reviewed/No Change	Originating Department:	Did this Policy Replace Another Policy? Yes X No	If Yes, Old Policy Title:
8/99, 5/00, 9/22/04 12/04, 12/06, 11/24/08	5/02, 8/02, 8/24/09, 2/22/10	HIM		Confidentiality – Release of Information From Patient's Medical Record

3. Contractors who have a Business Associate Agreement and access computer systems from outside CFVHS may be waived from signing the Agreement.
4. Entities that need access to the computer system but CFVHS does not have a contractual agreement are to sign a Non-Disclosure Statement and other documents requested by IST.

AUTHORITY TO AUDIT:

CFVHS has the right to audit any aspects of the computer system, including employee e-mail, to monitor compliance with this policy. Employees are not to have the expectation of privacy in anything they create, send, or receive on the computer. The computer and telecommunication systems belong to CFVHS and are used for CFVHS business (see Auditing Computer and Communication Devices Policy). Accounts may be disabled when a security/password violation occurs.

ELECTRONIC MAIL USE:

Users are to use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may be reviewed by others (see Electronic Mail Policy).

DESCRIPTION OF COMMON SECURITY VIOLATIONS:

1. Password Sharing: Sharing one's password with another, even as a matter of convenience and expediency is against CFVHS policy (see Password Policy).
2. Sticky Notes: An obvious compromise to security is writing one's password on a "sticky note" and placing it on or near the computer. Passwords are not written or placed in areas where they are accessible by other individuals (see Password Policy).
3. Browsing: Browsing a record or file, including those related to patients, employees, or health system financial data, to satisfy a personal curiosity is against CFVHS policy. This includes the employee's own and family member records.
4. Failing to Log Off: Workforce members are accountable for activity that is performed under their User ID and password.
5. Printed Information: Printed information of a confidential nature is carefully secured. Unneeded documents are shredded.
6. Software Copies: Copying licensed software, except for backup purposes, is not allowed. Users are to comply with software licenses, copyrights, and other state and federal laws governing intellectual property.
7. Restricted Area: Using an employee badge to access restricted areas to circumvent visitor policies.