

Mayo Clinic Arizona

Administrative Policies: Allied Health Staff

POLICY TITLE: Confidentiality: Patient and Employee Information

DATE EFFECTIVE: January 8, 2002

POLICY NUMBER: 1180

DATE REVISED: April 1, 2003

PURPOSE: To clarify Mayo's expectation of confidentiality concerning patient and employee information.

POLICY: To respect the sanctity of medical and business information.

PROCEDURES: Definitions

Archived Medical Record: The Archived Medical Record is the documentation of healthcare services provided to an individual. The Archived Medical Record is composed of a pre-defined set of documents that are used to respond to requests for the release of information (See Patient Care Policy - Medical Record Services Policy #2010 - The Electronic Medical Record and the Archived Medical Record). The Archived Medical Record does not include billing records, quality assurance or other peer review information or documents.

Protected Health Information (PHI): Any health information or demographic information that identifies a patient. See Patient Care Policy - HIPPA Policy #2024 - Identifying Protected Health Information for more details.

Obligation

Employees, volunteers and appointees have an obligation to conduct themselves in accordance with the principle of keeping all information concerning patients confidential. Staff members are to refrain from revealing personal or confidential information concerning other individuals or business operations, unless such use or disclosure is supported by legitimate business purpose. Carelessness or intentional acts leading to the release or misuse of confidential information is unethical and may result in legal action against the individual and/or Mayo.

The use of overhead paging to locate patients, guests, and/or Mayo employees is strongly discouraged. The use of such paging is disruptive to patient care and may potentially compromise the confidentiality of the person's presence at Mayo.

Confidentiality: Patient and Employee Information

Mayo allied staff and volunteers sign a Confidentiality and Computer Information Usage Agreement on their first day of employment or service. The Agreement should be re-circulated as needed to remind these individuals of their duty to maintain confidentiality.

Unauthorized use or release of confidential information at Mayo may be cause for corrective action up to and including termination of employment.

PATIENT INFORMATION - USE OF MEDICAL RECORDS

- The long-standing principle of confidentiality regarding protected health information must be maintained. The protected health information is used only for medical, research, education or other institutional purposes. MCS employees may access protected health information only when they are directly involved in the care of the patient and/or are responsible for an administrative function associated with the patient's care. The unauthorized handling or disclosure of protected health information can present serious ethical and legal problems.
- Certain types of protected health information such as alcohol and drug abuse treatment, psychiatric information, and HIV or other communicable disease information have federal or state statutory/regulatory protection. These laws must be complied with before such information is released.
- Physicians and other designated healthcare providers are encouraged to discuss the contents of the medical record with the patient in a manner and to the extent conducive to the physician-patient relationship and the patient's well being. Physicians should not encourage MCS employees to access their health information independently; test results and other personal health information are conveyed to MCS employees in the same manner as any other MCS patient.
- MCS employees, like all other patients, have the right to access their own medical records. Mayo has the responsibility to control, secure, and maintain all information contained in the MCS Archived Medical Record.
- Employees wishing to access (either "on-line" viewing and/or paper copies) their own medical records are required to make that request through the Medical Records Department. Medical Records staff will accommodate the request in accordance with the policies documented in Patient Care Policy - HIPPA Policy #1000 - Patient Requests for Records and Patient Care Policy #11024 - In-Patient Access for Medical Records. The appropriate authorization will be obtained and

Confidentiality: Patient and Employee Information

the employee will be provided with the requested information (either paper copies or access to a PC for “on-line” viewing). Employees are strongly discouraged from accessing their medical information prior to communication with/from their physician.

Employees with concerns related to the inappropriate access of their medical information should address those concerns with the Medical Records Department or their designated Human Resources representative. When deemed appropriate, an audit of the employee’s medical records will be requested by Medical Records or Human Resources to determine who has accessed the records. The discovery of inappropriate access will be reviewed by Human Resources. The employee who raised the concern will be advised that the audit has been completed, but will not be informed of any individual results.

- Employees may not access the protected health information (either "on-line" viewing and/or paper copies) of family members without the appropriate patient authorization. Requests for such access are handled through the Medical Records Department. (See HIPPA Policy #2000 - Use and Disclosure of Protected Health Information Requiring Patient Authorization).

EMPLOYEE INFORMATION

- Information concerning an employee's employment application, home address, telephone number, health information, reference information, credit information, salary, benefit information, performance evaluations and other related information is contained in the employer's file on each employee. These files and information are considered confidential. Human Resources releases information only to individuals who are authorized to receive it and who have a legitimate inquiry.
- Employees with access to such information may only use or divulge the information for legitimate business purposes.
- All requests for employment references are to be referred to Human Resources.
- The identities of job applicants are considered confidential and are not to be discussed with persons outside Mayo--except authorized references.
- It is the responsibility of persons who have possession of confidential employee information to maintain confidentiality of such records, and for proper disposal of records, documents and reports containing employee information.

COMPUTER SYSTEM ACCESS AND COMPUTER STORED RECORDS

- Computer records are accessed only for legitimate professional and/or Mayo business purposes.
- Each work unit is responsible for establishing procedures to ensure confidentiality of on-line information and computer-generated reports. Procedures may be required at the level of production, distribution, storage, collection and disposal of confidential reports. Suspected violations are reported to the supervisor, Administration, or to Security.