Regions Hospital®
HealthPartners®

CONFIDENTIALITY OF PATIENT/MEMBER INFORMATION EMPLOYEE ACCESS AND USE POLICY	**Manual:** Human Resources
	Number: RH-HR-HR-60-10-32
	Origination Date: August 2005
	Effective Date August 2005

I. PURPOSE

The purpose of this policy is to provide employees with specific guidance and expectations regarding the appropriate access to and use of "Protected Information" in order to perform their work. The guidance and expectations are pursuant to the Privacy Policy, which sets forth Regions Hospital overall policies regarding the protection of Protected Information.

II. DEFINITIONS

Protected Information: demographic, health or financial information that:

- Identifies (or could reasonably be used to identify) a patient or member, and is not generally known by or made available to the public;
- Is collected or received by or on behalf Regions Hospital (or any related organization) from a member (or his/her authorized representative), a patient (or his/her authorized representative), a member's or patient's health care provider or his/her agents, or a member's or patient's third party payer or health plan sponsor or his/her agents and;
- Relates to or facilitates the past, present or future physical or mental health condition of the member or patient, or the past, present or future provision of health care to the member or patient.

Protected Information includes, but is not limited to:

A. Information contained in medical, dental, eye, mental health, or other patient charts
B. Information contained in Health Plan files, e.g., Claims, Membership Accounting, Member Services etc.
C. Information contained in electronic systems and databases, e.g., electronic medical or dental records, Claims databases, Patient Accounting databases, membership accounting databases, Member Services databases, etc.
D. Appointment schedules
E. Other Protected Information maintained by RHSC, Inc. in conducting its business.

Protected Information may be recorded or unrecorded, oral, written, or electronically stored.

III. POLICY

Employees shall access Protected Information only to the extent necessary to perform their assigned duties. Employees must not use Protected Information for their individual or personal use except as specifically provided in this policy. In addition to compliance with this policy, an employee must comply with any policies, procedures, or protocols that are established for the employee's specific job and/or area.

All employees must exercise every reasonable precaution in safeguarding Protected Information in their possession or control. This includes, but is not limited to:

A. Keeping confidential patient/member charts and other confidential documents and

information where they will not be readily visible or accessible by unauthorized persons.

B. Not conducting conversations involving Protected Information where other employees or patients/members can overhear them (e.g., elevators, hallways, common areas, break rooms etc).
C. Disposing of documents that contain Protected information in an appropriate manner designed to preserve confidentiality (e.g., confidential document destruction containers, shredding.

COMMUNICATING PROTECTED INFORMATION

Employees must not discuss or communicate Protected Information with any other person, including a co-worker or organization, unless it is necessary in the performance of assigned duties. Protected Information must not be disclosed to parties outside the organization without appropriate written patient or member consent or authorization or as otherwise permitted in accordance with the Privacy Guidelines established pursuant to the Privacy Policy or other written privacy procedures established by the employee's department.

MONITORING OF PROTECTED INFORMATION

Employee access to Regions Hospital information systems, databases and files may be monitored on a regular or occasional basis.

EMPLOYEE ACCESS TO HER/HIS PROTECTED INFORMATION

Employees may ***on a limited basis,*** access their own Protected Information (e.g., own medical or dental record, appointment schedule information, pharmacy information, claims information, etc.) through Regions Hospital system's or files. However, such personal access shall only be on an incidental and occasional basis and shall not interfere with normal business activities or adversely impact the employee's or a co-worker's job performance. In addition, employees may not modify, print, copy, or forward their Protected Information or in any way perform transactions involving their own Protected Information. Thus, employee's access to their own Protected Information via Regions Hospital systems is permitted on a ***view only*** basis.

An employee may not use employment at Regions Hospital to access her/his Protected Information either directly or indirectly by asking another employee to access this Protected Information. An employee's ability or permission to access any Employer system containing Protected Information is dependent upon whether that person's job responsibilities require such system access. Accordingly, employees may not request, or receive access rights to systems that contain her/his Protected Information for the purpose of viewing her/his information.

EMPLOYEE ACCESS TO PROTECTED INFORMATION OF FAMILY MEMBERS

Protected Information about employee's family members, including minor children, must be treated in the same manner as that of other patients/members. The employee may not gain access to a family member's Protected Information as a result of her/his employment with Regions Hospital If an employee wishes to access the medical record, any medical information, laboratory results, appointment schedule information, pharmacy information, claims information, or any Protected Information of which a family member (including a minor child) is the subject, the employee may only access this information as would a non-employee patient member – for example, with required written authorization from the family member through Member Services or the clinic, or, in the case of information on-line, through member or patient portals.

An employee may not use employment at Regions Hospital to access the Protected Information of family members directly or indirectly by asking another employee to access Protected Information.

EMPLOYEE ACCESS TO PROTECTED INFORMATION OF CO-WORKERS

Protected Information about employees of Regions Hospital must be treated in the same manner as that of other patients/members. The employee may not gain access to another employee of Regions Hospital confidential patient/member information as a result of her/ his employment with Regions Hospital Employees may only access such Protected Information if it is necessary in the

performance of the employee's assigned duties.

EMPLOYEE ACCESS TO PROTECTED INFORMATION FOR TRAINING
Employees may not access or use Protected Information of family members or co-workers for training purposes, except with the written authorization of the family member/co-worker and with the express approval of the employee's supervisor.

Several of Regions Hospital information systems and databases contain built-in security functions to automatically monitor inappropriate access to Protected Information and supervisors/mangers receive reports on such access. Systems without automatic security functions may be monitored manually. Departments may institute special operating procedures for managing Protected Information of co-workers.

DISTRIBUTION
All new employees are informed about confidentiality and this Policy during Welcome Day and shown where to access this Policy in Compliance 360. Employees must sign the Orientation Outline indicating that the employee has received information on confidentiality.

If a new employee does not attend Welcome Day, this will be covered during a 1:1 session with Human Resources. The Employee must sign the Orientation Outline as stated above. The Orientation Outline will be retained in the employee's personnel file in Human Resources.

SUPERVISOR/MANAGER RESPONSIBILITY
Supervisors/managers are responsible for ensuring that all employees are aware of this Policy and for periodically reviewing this Policy with employees under their supervision.

It is recommended that for employees whose job requires regular access to Protected Information this Policy be reviewed at least on a yearly basis and that the supervisor/manager have the employee sign the Standards of Conduct Form on a yearly basis.

Supervisors/managers are responsible for reviewing and monitoring reports regarding employees' access to Protected Information.

Supervisors/managers are responsible for the daily administration of this Policy.

IV. COMPLIANCE
Failure to comply with this policy or procedures may result in disciplinary action, up to and including termination.

V. ATTACHMENTS
NA

VI. OTHER RESOURCES
Privacy and Protection of Patient and Member Information ("Privacy Policy")
Regions Hospital Code of Conduct (located on myPartner)
Discipline for Breeches of Privacy and Privacy Policies: RH-HR-HR-60-10-31

VII. APPROVAL(s)

Kim Egan
Executive Director, Human Resources