Regions Hospital
HealthPartners

Subject	Attachments
HIPAA SECURITY POLICY	☐ Yes X No
Key words	**Number** RH-HR-HR-60:10:30
Category Human Resources (HR)	**Effective Date** April 21, 2005
Manual Human Resources	**Last Review Date** July 2016
Issued By Human Resources	**Next Review Date** July 2017
Applicable Applies to all probationary and regular employees of Regions Hospital, vendors, contractors and other members of the work force.	**Origination Date** April 21, 2005
	Retired Date NA
Review Responsibility Human Resources	**Contact** Human Resources

I. PURPOSE

The purpose of this Policy is to ensure that the Organization maintains a consistent, effective and well-communicated approach to HIPAA Security. We are committed to protecting Electronic Protected Health Information (EPHI) to help meet our mission of improving the health of our Members, our Patients and the community we serve. Accordingly, the Organization will take appropriate and reasonable steps to protect EPHI from inappropriate access, misuse and compromise in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations.

This Policy also provides a framework and standard for all business units of the Organization to use as they comply with Security Standards, and develop and maintain Security Controls within each business unit

II. POLICY

The Organization is committed to safeguarding EPHI to achieve our Mission. We will ensure that we maintain appropriate and effective Security Controls and oversight of our Security Controls, and we will adopt and implement consistent and clear disciplinary measures for breaches of this Policy.

Each business unit is required to adopt written procedures and operational practices to implement the requirements of this Policy unless that business unit already has in place written procedures that are more stringent than this Policy. Those procedures and practices must follow the established Security Standards and must address how each business unit will implement the following requirements:

1.0 Security Management. The Organization will establish Standards and reporting structures to manage security activities, including methods to effectively prevent, detect, contain and correct security violations. This will be accomplished by implementing processes for risk analysis and risk management, sanction policies, and procedures for the review of information system activity. The management and reporting of security activities will be documented in accordance with the Security Standards.

2.0 Workforce Security. The Organization will establish Standards to ensure that all Personnel have appropriate access to EPHI and that unauthorized Personnel are prevented from obtaining such access. This will be accomplished by implementing procedures to ensure Personnel have the appropriate level of access assigned and also by implementing termination procedures. Use of assets and resources that allow access to EPHI will be documented in accordance with the Security Standards.

3.0 Information Access Management. The Organization will establish Standards for authorizing access to EPHI. This will be accomplished by implementing procedures for access authorization, establishment and modification. Requests for access to EPHI and for modifications to access will require approval in accordance with the Security Standards.

4.0 Security Awareness and Training. The Organization will implement Security Awareness and Training for all Personnel to include topics such as password management and protection from malicious code.

5.0 Incident Response. The Organization will establish Standards to address security incidents. This will be accomplished by implementing processes and procedures to identify and respond to suspected or known incidents in addition to mitigating, to the extent practicable, harmful effects of known security incidents.

6.0 Contingency Planning, Business Continuity and Disaster Recovery. The Organization will establish and verify Contingency Planning, Business Continuity and Disaster Recovery plans in accordance with the Security Standards. These plans will include provisions for EPHI and other assets in accordance with the HIPAA Security Rule.

7.0 Business Associate Agreements. The Organization will ensure Business Associate Agreements include language to the effect that the Business Associate will appropriately safeguard EPHI in accordance with the HIPAA Security Rule.

8.0 Facility Access Controls. The Organization will establish Standards and Controls to limit physical access to EPHI and the facilities in which they are housed. This will be accomplished by implementing procedures for the facility security plan, access control and validation, and maintenance records. Access to and use of EPHI and facility resources will be in accordance with the Standards.

9.0 Workstation Use and Security. The Organization will establish Standards to address appropriate workstation use in addition to establishing Controls, to the extent practicable, that physically restrict access to EPHI to authorized users. Use of EPHI and resources will be in accordance with the Standards.

10.0 Device and Media Controls. The Organization will establish Standards that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of its facilities and the movement of these items within the facility. This will be accomplished by implementing procedures for disposal, media re-use, accountability and data backup and storage.

11.0 Access Controls. The Organization will establish Standards to permit only authorized access to EPHI. This will be accomplished by implementing Controls to network and system resources for unique user identification, emergency access, automatic logoff and encryption.

12.0 Audit Controls. The Organization will establish Standards and mechanisms to record and examine information system and network activity. Procedures for compliance audits, implementation assessments and verification of the Security Controls will be established and documented in accordance with the Security Standards.

13.0 Integrity Controls. The Organization will establish Standards and mechanisms to protect EPHI from improper alteration or destruction.

14.0 Person or Entity Authentication. The Organization will establish Standards and Controls to verify the identification of those who authenticate themselves to systems for access to EPHI.

15.0 Transmission Security. The Organization will establish Standards and measures to guard against unauthorized access to EPHI that are transmitted over an electronic communications network.

16.0 Implementation. The Organization will ensure that activities are undertaken to develop and implement this Policy, the established Security Standards and written procedures as operational practices in accordance with the Standards.

17.0 Oversight. The Security Officer will have the responsibility and authority to ensure that this Policy is followed, including, without limitation, by:

(a) developing this Policy and the Security Standards and presenting this Policy and the Security Standards to the Security Council for approval;

(b) ensuring that the procedures and practices developed by business units and operational areas are consistent with this Policy and the Standards;

(c) overseeing implementation of this Policy and the Security Standards; and

(d) developing and implementing a process for documenting decisions for applying the HIPAA Security requirements.

The Security Officer may delegate these responsibilities to appropriate Personnel or to other committees, as deemed appropriate, so long as the Security Officer retains ultimate accountability for his or her delegated actions.

18.0 Noncompliance. Personnel who violate the Security Policy or any Security Standard and/or its associated security procedures applicable to the individual, will be subject to disciplinary action. Disciplinary action, up to and including dismissal, will be imposed consistently and commensurate with the nature of the violation, Organizational practice, policies, procedures and collective bargaining agreements. Failure of a Business Associate or contractor / subcontractor to comply with applicable Security Policy, Security Standard(s) or procedural provisions may result in immediate termination of network and system access privileges and / or termination of the relationship, in accordance with the applicable Business Associate Agreement or other contract.

III. PROCEDURE(S)

At the time of the adoption of this Policy, the Organization recognizes that the accreditation, compliance and industry standards related to security are evolving and changing. Potential inconsistencies in these standards and requirements combined with the difficulties in establishing appropriate, necessary and reasonable Controls will pose challenges to the business units.

It is the Organization's intent and desire that the business units establish Security Controls that are, at a minimum, in compliance with the applicable industry standards and regulatory requirements and that these Controls are operational by the required effective dates.

To this end, each business unit will, in conjunction with the Security Officer and his or her designees, complete an assessment and implementation work plan to ensure compliance with this Policy and the established Security Standards. Each business unit will be expected to take reasonable steps to ensure compliance at the date practicable considering future effective dates for certain federal laws pertaining to information security protections.

IV. DEFINITIONS

For purposes of this Policy, the following definitions apply:

"Business Associate" means a person or entity that provides certain functions, services or other activities for or on behalf of the Organization and receives, generates, uses or discloses EPHI in connection with those activities. (Employees are not considered Business Associates.)

"Controls" or "Security Controls" means a combination of policies, standards, procedures and technical controls to achieve confidentiality, integrity, availability and physical security of EPHI.

"Electronic Protected Health Information" or "EPHI" means health information in electronic form that:

(1) (a) identifies (or could reasonably be used to identify) a Patient or Member; and
(b) is not generally known by or made available to the public; and

(2) (a) is collected or received by or on behalf of the Organization from
(i) a Member (or his or her authorized representative);
(ii) a Patient (or his or her authorized representative);
(iii) a Member's or Patient's health care provider or their agents; or
(iv) a Member's or Patient's third party payor or health plan sponsor or their agents; and
(b) 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.

"Member" means an individual who is enrolled in, or who has applied to be enrolled in, a health plan underwritten or administered by HealthPartners, Inc. or a related Organization.

"Organization" means Regions Hospital.

"Patient" means an individual who has received (or is scheduled to receive) health care treatment or professional consultation from the Organization, or whose treating provider has sought a professional consultation from the Organization regarding that individual.

"Personnel" or "Staff" means any employee or individual under contract or other arrangement with the Organization to act on its behalf. This includes union and non-union employees, officers, physicians, Board members and volunteers, and any student under the supervision of the foregoing.

"Security Council" means a committee made up of both business and corporate leaders to provide guidance and oversight to the HIPAA security project and related compliance activities.

"Security Officer" means the individual with assigned responsibility for the development, approval and implementation of this Policy.

"Security Standards" or "Standards" means approved and written business standards adopted by the Security Council to support this Policy.

V. COMPLIANCE

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

VI. ATTACHMENTS

VII. OTHER RESOURCES

References to Legal Standards:

45 CFR Parts 160, 162 & 164 (HIPAA Security Standards; Final Rule)
45 CFR Parts 160 & 164 (HIPAA Privacy Standards; Final Rule)
Minn. Stat. Chapter 13 (Minn. Data Practices Act)
Minn. Stat. § 325L.01-19 (Minnesota's Electronic Signatures Act)
15 USC 7001 (Federal Electronic Signatures Act)

Cross References to Other Policies:

Records Retention Policy – see Administration Policy Manual
Privacy Policies-see Administration Policy Manual

VIII. APPROVAL(S)

Kim Egan
Executive Director, Human Resources

IX. ENDORSEMENT

Human Resources Leadership Team