REGAL MEDICAL GROUP, INC.	**DEPARTMENT: Information Systems**	
	Procedure No**. IS006**	Effective Date: 10/01/2005
	Authored by: C. Halasey	Date: 10/01/2005
	Approved by: Exec Team	Date: 10/26/2005
	Reviewed by: Exec Team	Date: 10/10/2005
	Revised by: J. Haggard	Date: 09/29/2009 Version: V1
TITLE OF POLICY: Information Systems, Computer Management		

Purpose:

The purpose of this policy is to provide definition and outline the management of Regal Medical Group information systems and security of electronic (PHI) patient protected health information.

Scope:

This policy covers all Regal Medical Group Employees

Definitions

Protected Health Information (PHI):
Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards. This includes but is not limited to Individually Identifiable Health Information and any personal identification or information that includes social security numbers, driver license numbers, occupational information, addresses, email addresses, IP or MAC Addresses.

Individually Identifiable Health Information:
Any information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse; and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual.

Computer Systems:
Computers or communication devices or digital copier devices (including Fax machines and scanners) that are stand alone or connected to local or wide area networks, telephone lines, database storage or electronic records systems, Internet or email, or which emit or receive Radio-Frequency Identication Devices or tools, or which emit or receive GPS signals, or which emit or receive satellite data or content.~~.~~

Local Area Network:

A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users.

Network Attached Computer:
Any computer system (desktop, laptop or server) that is physically or wirelessly or electronically attached to a local or wide area network.

Workforce:
Regal's workforce may consist of employees, volunteers, contract workers, trainees and other persons who are in Regal Medical Group's facility on a regular course of business. This shall include independent contractors, and/or client's workers employed by Regal Medical Group Inc. or any of its facilities or related entities.

Member:
Any individual who is eligible to receive, or is receiving medical or health care services from or through ~~Regal Medical Group~~Regal Medical Group, Inc. or its affiliated or managed or controlled medical groups or .

Restricted Access:
Restricted access is the practice of limiting any computer user or system limited access to specific systems, applications, activities, or files.

Security Officer:
The individual designated by Regal Medical Group, Inc. to oversee all activities related to the development, implementation, maintenance of, and adherence to Regal Medical Group Inc.'s policies and procedures covering the electronic and physical security of, and access to, protected health information and other Regal Medical Group data in compliance with HIPAA and other federal and state laws and regulations. In the case of Regal Medical Group this individual would be the SVP of Information Systems as may change in individual name from time to time.

Media:
Backup tapes, hard drives, floppy diskettes, CDs, zip drives cartridges, USB drives, jump drives, optical drive, and paper hard copies or any other type of portable data device.

Policy:

Users computers will be automatically placed in suspend and require a password for access after a maximum period of 5 minutes of inactivity.

The IS departments shall spot check an audit trail of all accesses and changes to patient data on a regular basis and report violations to the Security Officer and appropriate staff as designated.

Access to Regal Medical Group networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of Regal Medical Group Security Officer and Information Systems policy for access.

Regal Medical Group assigned staff from Information Systems technology management shall backup data in accordance with Regal Medical Group Data Backup Policy.

Regal Medical Group Security Officer and Technology staff shall ensure that all media has been thoroughly sanitized of any patient data before the media is recycled or disposed of, pursuant to Regal Medical Group Policy for Disposal of PHI and Policy for Devise and Media Controls.

Access to media containing patient data shall be controlled through:

1. Access control lists to network media.
2. Physical access control to Regal Medical Group's hardware.
3. Purging Regal Medical Group's data on any type of media before it is recycled or discarded.
4. Storage of data on media that is backed up.

Virus protection for the Regal Medical Group network or computer systems shall be maintained by Regal Medical Group Security Officer, pursuant to Regal Medical Group Virus Prevention Policies.

Equipment that has not been purchased by, and is owned by, Regal Medical Group shall not be allowed to connect to the Regal Medical Group's network without the permission and authorization of the Security Officer and others as designated.

Software
Regal Medical Group Security Officer shall maintain a support contract with software vendor(s) to ensure uninterrupted support.

Regal Medical Group's workforce shall not load software, from any source, onto their assigned workstation or any other Regal Medical Group's equipment without authorization from the Security Officer. This includes but is not limited to software from the internet, a CD, or a floppy diskette. Software shall be loaded on workstations only by designated employees of Regal Medical Group Security Officer.

Regal Medical Group workstations shall be situated by Regal Medical Group Inc.'s Security Officer so as to prevent more than incidental observation of work product or other sensitive data.

Responsible Departments:
Information systems – maintains the primary responsibility for the security of all computer systems attaching to the Regal Medical Group's network.

All Department and Users – maintain secondary responsibility to insure that passwords, IDs and access that are issue by the Information Systems department are restricted only to the assigned users and not shared under any circumstances.

Regal Medical Group Inc.'s Security officer, office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

Procedure:
Any violation of the policy should be communicated to the Security officer or Information systems technology staff immediately. The IS department under the guidance of the Security officer will evaluate any violation and communicate the finding to the appropriate management and Human Resources The Security Officer will review the findings and take appropriate action which can and may include job performance action, discipline which may include termination based on the severity of the violation.

Acknowledgement for Receipt of Policy and Procedure by Employee or other person being given access to any aspect of Regal Medical Group Inc.'s IS system, its computer system, email service, and/or its local or wide area networks, security access system, or to its wireless voice or texting, or internet interfaces:

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

I have received a copy of the Appropriate Use of Company resource policy and understand that it is my responsibility to abide by the policy.

_____ _____

Employee signature Date

_____

Employee name (please print)

Acknowledgement:

I have received a copy of the Internet Use policy and understand that it is my responsibility to abide by the policy.

_____ _____

Employee signature Date

_____

Employee name (please print)

_____ _____

Human Resources Date