PURPOSE:

*Purpose of Information Security Policy*

The purpose of this document is to define the principles to which all Orange Regional Medical Center Physicians, staff, volunteers, students must adhere when handling information owned by or entrusted to Orange Regional Medical Center in any form. The principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support the Orange Regional Medical Center’s objectives,
- Ensuring that those requirements are effectively communicated to individuals who come in contact with such information, and
- Using, managing and distributing such information – in any form, electronic or physical - in a manner that is consistent with those requirements.

This policy describes in general terms the Information Security Policy of the Orange Regional Medical Center, which is also embodied in various policies developed by the IT dept and Corporate compliance.
PROCEDURES:

Goal of the Information Security Program

The goal of the Information Security Program is to ensure that the…

- Confidentiality,
- Password protection 90 days reset
- Integrity and
- Availability
- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD).
- In physical storage environments (e.g., offices, filing cabinets, drawers),
- In a person’s memory, etc.

Summary of Personal Responsibilities

While much of this policy document focuses on our legal obligations and the process of determining and communicating the sensitivity of information owned by or entrusted to the Orange Regional Medical Center, it also contains a number of requirements to which anyone who handles such information must adhere. In summary:

- You are responsible for your use or misuse of confidential information.
- You must not in any way divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of your professional activities.
- You must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, e
- You must safeguard any physical key, ID card or computer/network account that allows you to access confidential information. This includes creating computer passwords that are difficult to guess.
- You must render unusable confidential information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
- You must report any activities that you suspect may compromise confidential information to your immediate supervisor or to the Orange Regional Medical Center IT Security Officer
**General Principles**

**Accountability**

All information gathered and maintained by employees of Orange Regional Medical Center for the purpose of conducting Orange Regional Medical Center business is considered institutional information and, as such, each individual who uses, stores, processes, transfers, administers and/or maintains this information is responsible and held accountable for its appropriate use.

**Information Collections and the Responsibilities of Managers**

Orange Regional Medical Center held information must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws (see Appendix A), and with the information’s significance to the Orange Regional Medical Center and any individual whose information is collected. Achieving this objective requires that Orange Regional Medical Center information be segregated into logical collections (e.g., medical records, employee benefit data, payroll data, and that each collection is associated with an individual known as a “Manager” who must:

- Define the collection’s requirements for confidentiality, integrity and availability
- Convey the collection’s requirements in writing to the managers of departments that will have access to the collection,

- Work with Department Heads to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).

The manager of a logical information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with such information. Each Manager may designate one or more individuals on his or her staff to perform the above duties. However, the Manager retains ultimate responsibility for their actions.

**Responsibilities of Department Heads**

Department Heads are required to:

- Understand the security-related requirements for the information collections used within their respective departments by working with the appropriate Managers.

- Effectively communicate any restrictions to those who use, administer, process, store or transfer the information in any form, physical or electronic.

- Ensure that each staff member understands his or her information security-related responsibilities and acknowledges that he or she understands and intends to comply with those requirements.

- Report any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt or destroy
User Responsibilities

Protecting Information Wherever It Is Located

Each individual who has access to information owned by or entrusted to the Orange Regional Medical Center is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by its Manager, wherever the information is located, i.e.,

- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks (data and voice),
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
- In physical storage environments (e.g., offices, filing cabinets, drawers),
- In a person’s memory, etc.

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained. Any individual who has been given a physical key, ID card or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network accounts should be difficult to guess (see “Password Policy” document for guidelines). Furthermore, passwords should never be shared or recorded and stored in a location that is easily accessible by others. Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be reported to the appropriate authorities immediately. The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

Diligence Concerning Information Associated with “Identity Theft”

Identity theft is a serious and growing problem in our society. Anyone who can obtain certain pieces of information about an individual can open credit cards, take out loans, create forged documents or steal assets in the individual’s name. Being sensitive to the identity theft threat, the Orange Regional Medical Center requires that extra precaution be taken when collecting, using and storing non-public “personally identifiable” information, such as;

- Social Security Number,
- Date of birth,
- Place of birth,
- Mother’s maiden name,
- Credit card numbers,
- Bank account numbers,
- Income tax records, and
Drivers license numbers

Collection and use of any of the above pieces of information should be limited to situations where there is legitimate business need and no reasonable alternative. Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorize individuals on a need to know basis.

Limitations on Sharing Personally Identifying Information

All non-public information gathered and maintained by employees of Orange Regional Medical Center, for the purpose of conducting Orange Regional Medical Center business, that personally identifies any living or deceased individual – names and other personal information pertaining to individual students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – is considered “confidential” unless otherwise specified by this document or by the appropriate Manager or designee. Such information associated with an individual may only be shared with:

- The individual with respect to whom the information is maintained,
- Persons designated in writing by that individual,
- Orange Regional Medical Center employees and representatives (included selected volunteers) who need access to such information for legitimate Orange Regional Medical Center business or to support the processing of such information, and who are authorized by the appropriate manager or designate,
  - Governmental agencies to which the Orange Regional Medical Center has a legal obligation to provide such information,
  - Orange Regional Medical Center-contracted organizations (e.g., health insurers, etc.) that:
    - Require such information to deliver their services on behalf of the Orange Regional Medical Center,
    - Are authorized by the appropriate Manager, and
    - Are bound by appropriate, non-disclosure agreements. An organization receiving non-public financial information must execute a Confidential Information Agreement (See Appendices F, G and H).

Is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by its Manager, wherever the information is located, i.e.,
- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks (data and voice),
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
- In physical storage environments (e.g., offices, filing cabinets, drawers),

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must ensure that information with maximum protection until its requirements can be ascertained. Any individual who has been given a physical key, ID card or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all
activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network accounts should be difficult to guess (see “Password Policy” document for guidelines). Furthermore, passwords should never be shared or recorded and stored in a location that is easily accessible by others. Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be reported to the appropriate authorities immediately. The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

**Exchanging Information via E-Mail or Other Network Facilities**
Electronic mail (e-mail) may in some situations be considered an insecure mechanism for exchanging information. The privacy of information contained within e-mail messages can be exposed, especially when either the sender or any of the recipients are off-campus or utilize a wireless network connection. The use of mechanisms that exchange information in a readable form, such as “ftp”, “chat” and “instant messaging”, between on- and off-campus computers also places confidential information at risk. If information, deemed by its Information Guardian as “confidential” or “highly confidential”, must be exchanged with an individual or entity off-campus using e-mail or any other network facility that transfers data, it must be encrypted using a hardware- or software-based (ZixCorp) mechanism approved by the Information Technology. All business-related e-mail containing “confidential” or “highly confidential” information sent to recipients who are not in the “ormc.org and ghvhs.org” domain must include the following disclaimer: “This electronic communication, including any attached documents, may contain confidential and/or legally privileged information that is intended only for use by the recipient(s) named above. If you have received this communication in error, please notify the sender immediately and delete the communication and any attachments.”

**Discarding Information**
Physical documents containing information that has been classified as “confidential” or “highly confidential” by their managers and/or designates must be shredded using our approved vendor shredding device or shredding facility prior to being discarded. Any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, Zip disk, etc., that has been used to hold any kind of “confidential” or “highly confidential” information is shredded prior to being discarded or being transferred to any individual or entity who is not authorized to view such information. On such media, the mere deletion of confidential data is not sufficient as deleted information is still accessible to individuals possessing any of a number of available software tools. Any non-erasable medium, such as a CD, optical disk, etc., that has been used to hold any kind of “confidential” or “highly confidential” information must be physically destroyed before being discarded. The Environmental Services Department provides secure bins for shredding materials when the volume to be discarded requires their assistance.

**Valid Uses of Aggregate Information**
Authorized users may analyze and aggregate institutional data. However, official, published reports that include such aggregate data may only be issued with the review and approval of the appropriate Information Manager. Similarly, sharing those reports with individuals or organizations for which the reports are not primarily intended requires the permission of the individual or office primarily responsible for the report.

**Subpoenas**
Authorized users are reminded that the full range of information collected on any living or deceased individual – students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries,
etc. – in hard copy or electronic form may be subpoenaed and entered into the public record of a court case. Appropriate discretion should therefore be exercised in the drafting of any document that will be stored in any Orange Regional Medical Center file. Employees who receive investigative subpoenas, court orders and other compulsory requests from law enforcement agencies that require the disclosure of Orange Regional Medical Center held information should contact the Office of General Counsel before taking any action.

**Reporting of Security Breaches or Suspicious Activity**
Any member of the Orange Regional Medical Center staff who comes across any evidence of information being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information must report such information to his or her immediate supervisor or to the Orange Regional Medical IT Security Officer. No one should take it upon himself or herself to investigate the matter further without the authorization of the Orange Regional Medical Center IT Security Officer or Compliance Officer/General Counsel.

References: