**Minimum Security Requirements for Ipadium Project**

Ipadium provides the medical division of CSIS with the capability to view and modify patient health information (PHI) from the master registration database from a tablet. To provide the secured network infrastructure from CSIS’s data vulnerable to hackers and other malware threats, the minimum security requirements are as follows:

1. **Access Control:**

Access control includes authorization and authentication, is the way of limiting access to a system or limiting connections to a network. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.

How it is useful for ipadium project:

In access control systems, users must present credentials to gain access. These credentials may come in many forms like fingerprints/retina scan or passwords which can't be transferred provides high security. So, this helps in ipadium project which allows an administrator to secure information and set privileges as to what information can be accessed, who can access it and at what time it can be accessed.

1. **Awareness and Training:**

Security awareness and training is a formal process which mainly focusses on educating employees about computer security.

* The main aim of awareness program is to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.
* Ensuring that the users are developing skills and knowledge to perform their jobs securely.
* Making sure that users clearly understand their responsibilities for protecting information resources.

How it is useful for ipadium project:

The users need to realize that most critical security threats come from internet access. This Security awareness training should educate users at a high level how monitoring tools are used and what information can be gathered by those tools. So that awareness and training is useful in ipadium project to track the threats and to protect PHI database by installing different software’s like firewalls and antivirus.

1. **Audit and Accountability:**

The purpose of this is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. A challenge for managers is to develop and implement systems, guidelines, and safeguards to identify and use available resources effectively and efficiently, with transparency and accountability. Accountability literally means to be held to account for, or to explain, one’s actions (or inaction) for which one has responsibility and authority.

How it is useful for ipadium project:

We should have an audit of login users (doctors) to know the status/security of accessing PHI database. IOS activities consist of internal auditing (assurance and advisory services) and examination of alleged wrongdoing (prevention, detection and investigative services).

1. **Configuration Management:**

Configuration management is the detailed recording and updating of information that describes an enterprise’s hardware and software. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. When a system needs a hardware or software upgrade, a computer technician can access the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.

How it is useful for ipadium project:

In IPadium project, PHI consists of ‘Network devices and infrastructure’ - Network devices such as routers, switches and firewalls are having specific controls that apply to segmentation of network traffic, inspection of traffic and encryption of traffic. So that updating of PHI database is needed.

* Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
* Health Insurance Portability and Accountability Act.
* National Institute of Standards and Technology Special Publication 800-41, Revision1, Guidelines on Firewalls and Firewall Policy, September 2009.
* NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, provides guidelines on how to establish and conduct an effective information security functional testing program.

1. **Contingency planning:**

Contingency planning in an organization refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption.

How it is useful for ipadium project:

PHI database needs Contingency planning for assessing the situation and to identify risks which is useful in ipadium project.

* Federal Information Security Management Act (FISMA) of 2002.
* OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
* Federal Continuity Directive (FCD)-1, Federal Executive Branch National Continuity Program and Requirements, February 2008.
* National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, National Continuity Policy, May 2007.
* National Continuity Policy Implementation Plan, August 2007.
* National Response Framework, March 22, 2008.

1. **Incident Response:**

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. The concept of computer security incident response has become widely accepted and implemented.

How it is useful for ipadium project:

By incident response capability the appropriate actions/decisions are taken by responding to incidents systematically. Incident response helps personnel to minimize loss or theft ofinformation and disruption of services caused by incidents.

* Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.
* The Federal Information Security Management Act (FISMA).

1. **Physical and Environmental Protection:**

An information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats.

How it is useful for ipadium project:

A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

In ipadium project, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor physical and environmental protection.

* E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
* Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
* Committee on National Security Systems Policy (CNSSP) No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, March 2007.

1. **Risk Assessment:**

Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

How it is useful for ipadium project:

Risk assessment is one of the important requirement in ipadium project to provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement them. Since risks and threats change over time, it is important that the Organizations (Hospitals) periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected.

* It is consistent with the policies presented in Office of Management and Budget (OMB) Circular A-130, Appendix III, “Security of Federal Automated Information Resources”.
* The Computer Security Act (CSA) of 1987.
* The Government Information Security Reform Act of October 2000.

1. **System and information integrity:**

State of a system where it is performing its intended functions without being degraded by changes or disruptions in its internal or external environments.

Assurance that the data being accessed or read has neither been tampered with, nor been altered or damaged through a system error, since the time of the last authorized access.

How it is useful for ipadium project:

The System and Information Integrity is used for managing risks from system flaws or vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. So, the system and information integrity program helps in our Ipadium project to implement security best practices with regard to system configuration, security, and error handling.