Introduction

The availability, integrity and confidentiality of Protected Health Information ("PHI") is of the highest importance to *Any Medical Practice* (hereby referred to as "Medical Practice"), our patients, and our business partners. In support of the commitment to protecting PHI, Medical Practice has developed and published this Information Security Policy ("ISP").

Applicability

The ISP applies to all PHI and other confidential information and the electronic systems that process, store, and transmit this information.

Purpose

The purpose of this Information Security Policy is to:

- Define a framework to enable the implementation of appropriate security and policy controls to protect Medical Practice against unauthorized access, use or disclosure of PHI.
- Provide all employees, contractors and other users with a clear statement of their responsibilities with respect to the security of assets and information.

Relationship with Other Policies and Requirements

This Policy is intended to complement, rather than replace, other corporate policies (e.g., employee handbook), or federal, state, and local laws and regulations, codes, rules and Contractual requirements. The ISP preempts all other information security policies in the event the ISP and another security policy (e.g., departmental policy) contradict one another whereby adhering to one would violate the other. Where a departmental policy, standard or procedure has stricter controls, the department is allowed to use the more restrictive control.

Responsibilities

Employees, Contractors and Consultants

All Medical Practice employees, contractors and consultants are expected to support and abide by the ISP. More detailed Baseline Requirements and Standards ("BRS") supporting the ISP define specific actions and responsibilities.

It is the responsibility of all managers to ensure that employees, contractors and consultants are aware of the ISP and the BRS as applicable, enforce compliance with the ISP and BRS and report any non-compliance including suspected or known incidents.

ISP Review and Update Policy

The ISP and all supporting BRS shall be reviewed at least annually, either internally by a qualified professional or by a qualified third party. More frequent reviews may be necessary to account for new or modified regulatory requirements, contractual obligations or changes in the business.

The updated ISP, including a summary of changes, shall be made available to all employees and contractors no later than the date the changes take effect. Various communications such as emails, meetings, etc. shall be used to ensure all employees and applicable contractors are made aware of the changes.

Availability

The ISP and all supporting BRS will be made available to all employees and contractors administrator’s office.

Revision History

This section is required for all policy and procedure documents to maintain formal change control.

Revision #	Date of Changes	Managing Editor	Summary of Changes	Reason for Changes
1.0	10/1/2013	[Manager]	Document created	Establish formal ISP

Overview

Purpose

The purpose of these baseline requirements is to provide guidance on the requirements for the use of antivirus software, firewalls to safeguard against access from unauthorized users, and password protected encryption on all desktops and laptops to minimize the threat of loss, theft of the device itself, and any security risks of sensitive information.

Regulatory Reference: *45 CFR 164.308(a)(4)(i), 45 CFR 164.308(a)(4)(ii)(B), 45 CFR 164.310(b)*

Baseline Requirements

General

- All Medical Practice desktops and laptops must run Medical Practice-approved anti-virus software.
- Anti-virus software must be set to scan for updates and monitored to ensure that they are applied within 24 hours of availability.
- All Medical Practice desktops and laptops must not be tampered with so as to disable antivirus software.
- Antivirus software must be configured to periodically scan files in storage, and to scan downloads from external sources as they are downloaded, opened, or executed.
- Any contractor or third party laptops that may be connected to the internal Medical Practice network must have confirmed updated antivirus software prior to connection to the network.
- All Medical Practice desktops and laptops must run a Medical Practice supported firewall.
- Firewalls must perform stateful packet inspection at a minimum.
- All Medical Practice desktops and laptops must be protected by boot passwords as well as disabling the boot options from alternate media (including but not limited to USB flash drive, CD, or floppy).
- All Medical Practice desktops and laptops containing PHI must be encrypted.
- All Medical Practice desktops and laptops devices must be secured with a password protected screen saver when left unattended and must be configured to automatically lock after a predefined period of inactivity.
- All users must take all reasonable steps to protect against the installation of unlicensed or malicious software.

Revision History

This section is required for all policy and procedure documents to maintain formal change control.

Revision #	Date of Changes	Managing Editor	Summary of Changes	Reason for Changes
1.0	10/1/2013	[Manager]	Document created	Establish formal BRS

Overview

Purpose

The purpose of these baseline requirements is to provide guidance regarding the use of removable media devices (e.g., CDs, DVDs, and USB drives) to maintain the security of information and to help prevent unauthorized disclosures, modification, removal or destruction of assets.

Regulatory Reference: *45 CFR 164.310(d)(1), 45 CFR 164.312(a)(2)(iv), 45 CFR 164.312(e)(1), 45 CFR 164.312(e)(2)(i-ii)*

Baseline Requirements

General

- Medical Practice must provide encrypted removable media devices (e.g., CDs, DVDs, and USB drives) if circumstances require copying data as part of business operations.
- Saving data to removable media will only be permitted using Medical Practice owned/purchased media. Saving data to media provided by any other source (personal, client, auditor, found in the parking lot, etc.) is not authorized.
- When no longer required, the contents of any removable media must be made unrecoverable and in accordance with approved data destruction standards (see 7.0 Secure Disposal).

Revision History

This section is required for all policy and procedure documents to maintain formal change control.

Revision #	Date of Changes	Managing Editor	Summary of Changes	Reason for Changes
1.0	10/1/2013	[Manager]	Document created	Establish formal BRS

This baseline requirement is the minimum level of control necessary for adherence to the information security policies and is not intended to be all inclusive of regulatory, legal, or contractual requirements.

Overview

Purpose

The purpose of these baseline requirements is to provide guidance regarding safeguards for protecting data, software, and hardware contained on mobile devices (e.g., smart phones, tablets) to minimize the threat of loss or theft of the device itself and any sensitive information contained therein.

Regulatory Reference: *45 CFR 164.310(d)(1), 45 CFR 164.312(a)(2)(iv), 45 CFR 164.312(e)(1), 45 CFR 164.312(e)(2)(i-ii)*

Baseline Requirements

General

- Medical Practice does not support mobile device computing at this time.
- No data shall be stored or transmitted to mobile devices
- Users are not permitted to bypass or attempt to bypass security protections or connect mobile computing devices to the Medical Practice network or Medical Practice communication systems.
- Medical Practice management must ensure that their staff adheres to the requirements outlined in this policy.

This baseline requirement is the minimum level of control necessary for adherence to the information security policies and is not intended to be all inclusive of regulatory, legal, or contractual requirements.

Revision History

This section is required for all policy and procedure documents to maintain formal change control.

Revision #	Date of Changes	Managing Editor	Summary of Changes	Reason for Changes
1.0	10/1/2013	[Manager]	Document created	Establish formal BRS