Internet Connections

Introduction

While the Internet is an important business resource, it is not a secure environment. Unencrypted Internet traffic can be easily captured and reviewed. Connecting to the Internet, or using it to connect from remote locations to FMCNA systems, increases the risk of inappropriate access to PHI/PI.

Using the Internet to access the Company's systems, without the appropriate controls, could allow Company information to be accessed by unauthorized individuals.

Unauthorized internet connections could provide undetected pathways for intruders to bypass important network controls (e.g.- Corporate firewalls) architected by Network Security to protect PI/PHI.

This section defines tasks and responsibilities to minimize those risks.

Internet Connections: IS/IT Responsibilities

IS/IT is responsible for the following safeguards:

- Provide network connections from FMCNA facilities to the Internet to support the requirements of the businesses.
- Provide the appropriate firewalls and network-based controls to prevent unauthorized access from the Internet to FMCNA systems.
- Provide a secure VPN solution for authorized users to safely access FMCNA systems from remote locations over the Internet.
- Document all approved requests for VPN access.
- Develop and implement procedures for the immediate revocation of access on an employee's termination with the Company.
- Develop banners and reminders with Compliance and the Law Department and post them to notify users of their responsibilities when using the Internet, or when using FMCNA systems over the Internet.
- Select and implement content management controls (e.g.-Websense) that limit users' access to the Internet to web sites that the Company deems appropriate.
- Log and monitor user's access to web sites, providing reports to Management, Compliance or the Law Department as needed.

Continued on next page

Internet Connections, Continued

Internet Connections: User Responsibilities

Users must do the following in order to support the safeguards provided by IS/IT:

- Make all requests for additional Internet connections to network security.
- Go through IS/IT to get additional network connections or equipment, including wired hubs, wireless access points or dial-up access.
- Never connect personal network equipment like a wired hub or a wireless access point to the Company's network.
- Never install VPN or other software that would provide a virtual network connection to another Company's network.
- Use only the Company-provided VPN solution to access the Company's systems over the Internet from remote locations.