


COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES
POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Malicious Spyware	POLICY: 01-247
SECTION: Administration	EFFECTIVE DATE: 10-14-15
REFERENCE: 45 CFR Sections 164.308 (a) 164.312 (b), 164.312 (c) (1), 164.312 (c) (2)	PAGE: 1 of 4
AUTHORITY: Behavioral Health Director as the Local Mental Health Director/Alcohol and Drug Administrator	SUPERSEDES: New Policy
	APPROVED BY: 

PURPOSE: The purpose of this policy is to ensure that all information systems are protected against malicious code from web pages, email and other network based exploitation that could result in the compromise of confidentiality, integrity and availability of EPHI by computer viruses, worms, trojans, spyware, adware and rootkits.

NOTES: None

DEFINITIONS: Anti-virus software: Software that detects or prevents malicious software.

Device: A device is a unit of hardware, inside or outside the case or housing for the essential computer functions (the processor, memory, and data paths). A device is capable of providing input, receiving output, or both.

EPHI - Electronic Protected Health Information: refers to any protected health information (PHI) that is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulation and is produced, saved, transferred or received in an electronic form.

Firewalls: Special computer programs and hardware that are set up on a network to prevent and intruder from stealing or destroying data.

Malicious software or malware: A type of software that includes ways of attacking data integrity, the system itself or the confidentiality of the data. Malicious software includes viruses, virus variants, worms, hoaxes, and trojan horses.

Network: A group of computers (workstations) and associated devices connected by a communications channel to share information files and other resources between multiple workforce members.

Protected Health Information (PHI): Individually identifiable information relating to past, present, or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual transmitted or maintained in any form or medium including oral, written, or electronic communication.

Server: A computer device on a network that manages network resources.

Trojan horse: A program in which malicious or harmful code is contained inside an apparently harmless programming or data.

Virus: A piece of code, typically disguised, that causes an unexpected and other undesirable event. Viruses are frequently designed to automatically spread to other computers. They can be transmitted by numerous methods; as email attachments, as downloads, and on floppy disks or CDs.

Vulnerability: A flaw or weakness in system security procedures, design, implementation or internal controls that can be exploited by a threat and result in misuse or abuse of EPHI.

Workstation: An electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, an electronic media stored in its immediate environment.

Worm: A piece of code, usually disguised, that spread itself by attacking and copying itself to other machines. Some worms carry destructive payloads that delete files or distribute files; others alter Web pages or launch denial of service attacks

POLICY OWNER: Security Officer

POLICY: It is critical that each device in the enterprise is protected to the maximum degree possible from attack using malicious software and scripts. The department's network is behind a firewall configured to prevent malicious connections attempting to exploit known vulnerabilities. The firewall uses Network Address Translation (NAT) to ensure that internal devices are not visible from the internet unless explicitly configured. Servers, workstations and other devices rely on software that is currently supported by the vendor and subject to security updates and patches to address emerging threats and vulnerabilities. Patches are installed either in a scheduled, periodic patch process, or an automatic patch feed if available.

Support staff plays an important role in preventing and detecting malicious code. The staff is provided with training materials that help them to 1) maintain the security of devices and software that they use, 2) identify symptoms of malicious code and 3) follow the proper procedures in the event of malicious code.

This policy applies to all devices and systems including network infrastructure, networked appliances (such as medical equipment) and all forms of workstations and servers.

Standards

1. Each enterprise network shall be isolated from the internet using a NAT firewall
2. Each system including but not limited to servers, workstations, laptops, mobile devices, should have:
 - * All applicable vendor supplied security patches installed within 60 days of release
 - * All supported Anti-Virus/Anti-Spyware/Anti-Malware software package installed, patched and operational
 - * Current Anti-Virus signatures that are no more than 48 hours behind release by the vendor
 - * Anti-Virus package should be configured to:
 - Scan all incoming email and attachments
 - Scan the entire disk daily
 - * All systems shall be checked each year to verify that:
 - All software is supported by the vendor with security updates to close known vulnerabilities

- Anti-Virus software is operational and up to date
 - All quarantined files have been removed
 - All required patches have been installed
 - * Configuration settings that meet any applicable requirements of the System Configuration policy
3. Each staff member shall be trained in the symptoms of malicious software, antivirus/antispyware alerts and the incident reporting process.
 4. Procedures should be implemented to ensure that the above standards are met.

Related policies and Regulations:

Policies:

- 01-86 HIPAA Security and Privacy Training
- 01-229 Security and Privacy Management

Regulations:

1. 45 CFR Section 164.308 (a)(5)(ii)(B) Implement Protection from malicious software (Addressable). Procedures for guarding against, detecting and reporting malicious software.
2. 45 CFR Section 164.312 (b) Standard. **Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
3. 45 CFR Section 164.312 (c)(I) Standard. **Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
4. 45 CFR Section 164.312 (c)(2) Standard: **Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.