CHS Community Health Systems

Removable Media Policy

Sponsor: VP of Information Systems	**Area:** Information Systems
Effective Date:	**Description:** Removable Media Policy
Next Review Date:	**Policy Number:** IS-SEC-018 rev. 1
Supersedes: Removable Media Use Policy	**Page:** 1 of 2

Purpose:

The purpose of this policy is to outline the acceptable use of removable media at CHS entities.

Scope:

New technologies in secondary storage media devices have introduced the need to clarify current information assurance policy, as these devices pose additional risk to CHS information systems. Operational benefits of highly portable, reusable and removable secondary storage media devices are acknowledged. This policy refers to removable media as defined below (see *Definitions*).

Policy:

In general, users are not to use any writable media (USB drives, CD/DVD, etc.) on CHS devices or connected to the CHS Network. If there is job-related need to use writable removable media, it must be approved by the user's manager. Use or connection of personally-owned or non-CHS issued removable media with CHS computing devices is prohibited.

It is strictly prohibited to use removable media to store, access, transport, or replicate PHI or other confidential information. If there is job-related need to exchange PHI or confidential information with a vendor or business partner via removable media, CHS must have a non-disclosure and business associate agreement in place with that vendor/business partner, and the user must have permission from their manager. If the removable media is sent via courier (US Mail, FedEx, etc.), the package must be tamper-evident, tracked via the courier (date and time stamp with location), and CHS shall request the signature of the individual receiving the package, e.g., certified mail or registered mail, with delivery confirmation and signature confirmation.

CHS reserves the right to audit removable media found in the workplace to ensure compliance with this policy.

Definitions:

Removable Media - Any device that can be connected to a workstation or other computing device via cable, universal serial bus (USB), PCMCIA, or other connector for the purpose of storing data. Examples include: USB Flash Drives, Thumb drives, Bluetooth-enabled devices, Jump drives", ATA Flash Devices, CDs, DVDs, floppy disks or other similar removable storage devices.

Discipline:

Failure to comply with this policy may lead to disciplinary action up to and including termination.

References:

HIPAA Security Act 164.310(b) and (c) - Workstation Use & Security
HIPAA Security Act 164.310(d)(1) – Device & Media Controls
CMS Security Standard: Media Protection (MP)