Data Security Policy - Device and Media Control

PURPOSE

To provide principles and guidelines for device and media controls and safeguards at Organization, including endpoint and mobile devices.

SCOPE

- The Device and Media Control Policy will cover Organization's**:**
- Device, hardware, and media controls and handling
- Device, hardware, and media tracking and documentation
- Device, hardware, and media usage and disposal
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has and follows a process for managing physical devices, hardware, and media that contain sensitive or protected data, such as ePHI*.* The company tracks and documents all devices, hardware, or media in use at Organization, and stores this information in our *Asset Management Repository*. We may choose to use the Guard's Asset module for this purpose.

When necessary, additional training is provided to personnel and users that are responsible for managing and disposing of devices, hardware, and/or media.

Any instances of loss or theft of devices must be reported immediately.

Device, Hardware, and Media Management

Organization has and follows a process for onboarding new devices, hardware, or media into the environment. Devices must be configured and hardened to the level defined by the company before being used in a production environment. Devices are stored in secure physical locations. Devices, hardware, and media are tracked in the company's *Asset Management Repository*. We may choose to use the Guard's Asset module for this purpose.

Any devices that are re-used are sanitized of sensitive or protected data prior to re-use.

Device, Hardware, and Media Disposal

Organization has and follows processes for disposing of devices, hardware, and media, including those that house sensitive or protected information, such as ePHI*.* Disposal processes include the sanitization and removal of sensitive or protected data. Disposal of physical assets are conducted securely and tracked.

Devices, hardware, or media that contained ePHI must have ePHI rendered unusable, unreadable, or inaccessible for proper disposal.

Device, Hardware, and Media Tracking and Documentation

Organization has and follows processes for documenting devices, hardware, and media control activities. Documentation includes a chain of custody, which indicates the individual responsible for the device and the location of the device.

Organization retains any documentation related to the management of devices, hardware, and media, from procurement to disposal or decommissioning.

Device, Hardware, and Media Backups

Organization has adopted and follows a process for backing up sensitive or protected information, such as ePHI*,* in compliance with the HIPAA Security Rule.

PROCEDURES

Organization has set up a process to track all devices, hardware, media, and assets at the company in our *Asset Management Inventory* or Repository. The Guard has an Asset Module available for this use.

Any instances of loss or theft of devices must be reported immediately through the incident management reporting workflow.

Device, Hardware, and Media Management

When new devices, hardware, or media are added to the Organization’s environment, they are also added to the company’s *Asset Management Inventory*. The *Asset Management Inventory* should include the following details for each asset:

- Unique ID
- Serial number
- Operating system
- Database type
- IP address
- Production / Development / Test / QA
- Contains / Does not contain ePHI
- Asset name
- Department or business unit
- Owner
- Other important details

Devices are hardened to the configuration and integrity standards defined by the company for each asset type. Hardening involves configuring assets to a secure baseline. Hardening occurs before the asset is used in production environments. Device hardening and configurations are tracked or linked through the *Asset Management Inventory*.

Any physical assets are stored in secure, locked locations. These storage locations should only be accessed by workforce members authorized to handle physical devices, hardware, or media.

Device, Hardware, and Media Disposal

Organization has set up processes for disposing of devices, hardware, and media, including those that house sensitive or protected information, such as *ePHI.* The disposal process includes the sanitization, purging, or destruction of sensitive or protected information from the device, hardware, or media. Disposal processes are tracked in the *Asset Management Inventory* and ticketing system (or similar tool) as they occur.

Once devices, assets, or media are sanitized, the physical asset may need to be disposed of. Organization will use a secure disposal or destruction service to destroy any devices, hardware, or media that need to be physically destroyed, and retain certificates of destruction for physical assets destroyed.

Device, Hardware, and Media Tracking and Documentation

Organization has set up processes for tracking devices, hardware, and media, and documenting control activities. The *Asset Management Inventory* contains all key information about devices, hardware, and media in use at the company. A ticketing system or similar tool is in place for tracking the movement or disposal of devices, hardware, and media.

Documentation includes a chain of custody, which indicates the individual responsible for the device and the location of the device.

Devices, hardware, or media that contain or process sensitive or protected information must have a request and approval documented and tracked if the physical asset is moved from one facility to another.

Device, Hardware, and Media Backups

Organization has set up a process for creating exact copies or backups of sensitive or protected information, including ePHI. Backups are stored securely and encrypted to safeguard sensitive or protected data. Additional backup and recovery procedures can be found in The Guard under the Data Security Policy - Contingency Plan.

Definitions

Clearing

Clearing sanitizes data, protecting against simple, non-invasive data recovery techniques. Clearing is typically applied through standard Read/Write commands to the storage device. This may include rewriting with a new value or using a menu option to reset a device to the factory state (when rewriting is not supported). The data is then overwritten and verified. Most devices support some level of clearing sanitization. Clearing sanitization has a limit, however – it does not reach hidden areas or areas that cannot be addressed.

Purging

Purging applies techniques that render data recovery infeasible. Purging provides a more thorough level of sanitization than clearing and is used for more confidential data. Purging requires the removal of hidden drives, if these are present. Purging may not work on all firmware.

Destroying

Destroying renders target data recovery infeasible. Destroying also renders the media incapable of storing data afterward. “Destroying” includes a variety of techniques, such as shredding, incinerating, pulverizing, melting, and other physical techniques. These techniques may be necessary for drives that are already beyond all possible use or standard overwriting methods because of physical damage.

ROLES AND RESPONSIBILITIES

Device Owner: Responsible for handling assigned devices, hardware, or media. Ensures compliance with Organization’s policies and procedures.

FORMS/PLANS/DOCUMENTS

- Asset Management Repository or Inventory (The Guard’s Asset module can be used for this purpose.)

RELATED POLICIES OR PROCEDURES

- Data Security Policy - Contingency Plan

RELEVANT HIPAA REGULATIONS

- § 164.310(d)(1) *Device and media controls*
- § 164.310(d)(2)(i) *Disposal*
- § 164.310(d)(2)(ii) *Media reuse*
- § 164.310(d)(2)(iii) *Accountability*
- § 164.310(d)(2)(iv) *Data backup and storage*

RELEVANT SOC 2 CRITERIA

- CC2.1.1 *Identifies information requirements*
- CC2.1.4 *Maintains quality throughout processing*
- CC3.2.6 *Identifies and assesses criticality of information assets and identifies threats and vulnerabilities*
- CC6.1.1 *Identifies and manages the inventory of information assets*
- CC6.5.1 *Identifies data and software for disposal*
- CC6.5.2 *Removes data and software from entity control*
- CC6.7.3 *Protects removal media*
- CC6.7.4 *Protects mobile devices*