Media Sanitization and Disposal Policy **Reviewed July 5, 2018**

Purpose

The purpose of this policy is to protect College Data from unauthorized disclosure. This policy defines the requirements for ensuring College Data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to College Data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

Scope

This policy applies to all colleges, departments, administrative units, and affiliated organizations.

Effective Date

This policy became effective on August 1, 2013.

Authority

The Alabama College of Osteopathic Medicine requires all divisions to "establish policies and procedures for the sanitization of all media including hard copy and electronic." It also instructs institutions to use "the guidelines contained in NIST Special Publication 800-88 or an approved established industry best practice for higher education technical environments or institutions."

The Health Insurance Portability and Accountability Act of 1996 specifies requirements for disposal, media reuse, and accountability for electronic protected health information.

The Internal Revenue Service (IRS) Publication #175, Tax Information Security for Federal, State, and Local Agencies and Other Entities, specifies security controls for protecting the confidentiality of Federal Tax Information that includes media reuse and disposal.

Policy

To prevent unauthorized disclosure of College Data, media leaving control of the responsible department and destined for reuse or disposal must have all College Data purged in a manner that renders the data unrecoverable.

Media that will be reused within the department should likewise have all College Data purged to prevent unauthorized disclosure.

Media containing College Data authorized by the appropriate administrative head for transfer to individuals or organizations outside the College are exempt.

Definitions

1. Affiliated Organization - any organization associated with the College that uses college information technology resources to create, access, store or manage College Data to perform their business functions.

2. Confidential Data - Highly sensitive College Data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. See ACOM's Data Classification and Security Policy for an expanded definition and examples.

3. Degaussing - demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

4. Disintegration - A physically destructive method of sanitizing data; the act of separating into component parts.

5. HIPAA - Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

6. Incineration - A physically destructive method of sanitizing media; the act of burning completely to ashes.

7. Internal Data - College Data intended for internal College business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. See ACOM's Data Classification and Security Policy for an expanded definition and examples.

8.Media - material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

9. Media sanitization - the process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

10. Public Data - College Data explicitly or implicitly approved for distribution to the public without restriction. See ACOM's Data Classification and Security Policy for an expanded definition and examples.

11. Pulverization - A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

12. Purging - a media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

13. College Data - Any data related to Alabama College of Osteopathic Medicine ("College") functions that are a) stored on College information technology systems, b) maintained by ACOM faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

Roles and Responsibilities

The local department is responsible for ensuring that College Data are properly removed or destroyed from media before it leaves the control of the department for reuse or disposal.

Implementation Procedures

While the primary purpose of this policy is to protect non-public College Data (e.g., data classified either internal or confidential), it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge all College Data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the College, all College Data must be purged from the media before giving it to the third party.

Specific instructions for different types of media and regulations follow.

A. Electronic Storage Media (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.)

1. If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes.

2. Equipment that can store College Data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the College should have all data storage devices removed before disposition. If the equipment leaving College control must retain the data storage devices, all College Data must be properly purged.

3. The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.

4. Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

B. Paper-Based Media

1. Any paper-based or other hard copy media containing confidential College Data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the College for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").

2. Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

C. Optical Media (e.g., CDs and DVDs)

Optical media containing internal or confidential College Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

D. Smartphones, Personal Digital Assistants (PDAs), and other handheld devices

Mobile devices like Smartphones (e.g., Blackberry or Treo), PDAs, MP3 players, and even regular cell phones store information and often contain personal or other sensitive information. Any College Data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

E. Other Media Types

For other media and additional guidelines, refer to National Institute of Standards and Technology (NIST) Special Publication 800-88, table A-1 "Media Sanitization Decision Matrix," in Appendix A, Minimum Sanitization Recommendations for Media Containing Data.

F. Export controls

Media containing College Data in equipment that will be reused outside the United States must comply with export laws and regulations according to ACOM's Export Control Program.

G. Electronic Protected Health Information

ACOM units responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2).

H. Federal Tax Information

ACOM units handling Federal Tax Information must also have media sanitization and disposal policies and procedures in accordance with IRS Publication #175, Tax Information Security for Federal, State, and Local Agencies and Other Entities.

I. More Information

For more information about media sanitization and disposal, including suggested software tools for purging hard drives and other ACOM-specific resources and procedures.

Related Laws, Regulations, or Policies

1. ACOM Data Classification and Security Policy

2. Guidelines for Media Sanitization, NIST Special Publication 800-88
http://www.csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

3. HIPAA Final Security Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2)

4. IRS Publication #175, Tax Information Security for Federal, State, and Local Agencies and Other Entities. February 2007.http://www.irs.gov/pub/irs-pdf/p1075.pdf

Questions/Waivers

The Director of Information Systems is responsible for this policy. The Dean or designee must approve any exception to this policy or related procedures.

Questions should be directed to the Director of Information Systems.