Storing electronic media containing protected health information in off-site storage at Access facilities

University Records Management Guidelines

Requirements

In compliance with the rules and regulations of the federal Health Insurance Portability and Accountability Act (HIPAA) and University of Pittsburgh electronic data security policies, University of Pittsburgh units, offices, and departments utilizing off-site storage through accounts with Access Information Management are notified of the following:

1. Data drives, tapes or disks containing protected health information (PHI) as defined by the HIPAA Privacy Rule (45 CFR 164 § 501) and being sent to off-site storage facilities maintained by Access Information Management **must be encrypted** following guidelines issued by the Human Research Protection Office and the University's Computing Systems and Services Department.

2. University of Pittsburgh units, offices, and departments must contact the Office of the CIO concerning exceptions to the University's encryption security policies. Should an exception to said policies be granted, data drives, tapes or disks requiring off-site storage at Access facilities that are not encrypted following guidelines issued by the Human Research Protection Office and University's Computing Systems and Services Department must satisfy both of the following requirements:

2.a. Approval must be granted by the Chief Information Security Officer, Office of the CIO.

2.b. Official written notification documenting the transfer of storage of said non-encrypted data drives, tapes or disks submitted to Access Information Management.

Definitions

- **Health Insurance Portability and Accountability Act (HIPAA):** U.S. legislation passed in 1996 providing security and privacy provisions for the protection of medical health information.
- **Protected Health Information (PHI):** Individually identifiable health information. Protected Health Information shall have the same meaning as the term "protected health information" in 45 CFR §160.103 and HIPAA Privacy Rule 45 CFR 164 § 501. PHI includes electronic protected health information (EPHI).
- **Access Information Management:** The University of Pittsburgh's contracted vendor for secure off-site storage, destruction, and tape rotation services in conjunction with the university records management program. Formerly Business Records Management, LLC.
- **Encryption:** University of Pittsburgh PHI must be correctly protected and de-identified to appropriate NIST standards wherein they are unusable, unreadable, or indecipherable to unauthorized users.
- **De-identifying Health Information:** Identities cannot be readily ascertained. Please see CSSD guidelines.
- **U.S. Department of Health and Human Safety Certified Electronic Records Technology Standards:** HHS safe harbors guidance set forth "Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable," 45 C.F.R. part 170.

Resources

- CSSD Security Policies
- Human Research Protection Office (HRPO) Electronic Data Security Guidelines

  **The University of Pittsburgh Human Research Protection Office recommends EPHI be encrypted when "at-rest where other data is being stored and in-transit as the data is being moved from one location to another."*
- University of Pittsburgh Privacy Practices
- University of Pittsburgh Policy 07-02-06: Security of Electronic Medical Records – Compliance with the Health Insurance Portability and Accountability Act

  **Section 3.1.4 states: "…each Covered Component will ensure that security controls are in place to protect the integrity and confidentiality of EPHI… measures each Covered Component should address include: Encrypting EPHI that is transferred or stored on systems not controlled by the Covered Component."*
- University of Pittsburgh Policy 07-02-09: Proper Handling of Protected Health Information Outside of the University
- University of Pittsburgh Policy 10-02-06: University Administrative Compute Data (UACD) Security and Privacy
- University Records Management

Participating Offices

- Office of General Counsel
- Office of the Chief Information Officer
- University Records Management, ULS