Heller School for Social Policy and Management

Data Destruction Policy for Strictly Confidential Data

1. Definitions - For the purposes of this policy, 'Strictly Confidential data' means any data set that contains one or more HIPAA defined identifier. These include:
    - Names
    - All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
    - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90
    - Phone numbers
    - Fax numbers
    - E-mail addresses
    - Social Security numbers
    - Medical record number
    - Health plan beneficiary number
    - Any other account numbers
    - Certificate/license numbers
    - Vehicle identifiers
    - Device identification numbers
    - WEB URL's
    - Internet IP address numbers
    - Biometric identifiers (fingerprint, voice prints, retina scan, etc)
    - Full face photographs or comparable images
    - Any other unique number, characteristic or code.

    a. For the purposes of the policy, 'electronic and other media' shall include any non-paper material or media on which information can be stored or preserved, including, but not limited to, computer hard drives, zip drives, 'thumb' drives, floppy disks, UBS flash drives, memory sticks, magnetic tape, or other electromagnetic or electromechanical means of storing date, and includes optical storage media such as CDs or DVDs.

2. Oversight

The DUA Database Administrator has been designated as the entity responsible for oversight of destruction of secure data. The Administrator is responsible for questions regarding this policy, and should be contacted by any employee with questions regarding this policy. In addition, the Administrator shall be responsible for:

- Identifying employees who handle and dispose of secure data
- Providing training for employees regarding the requirements of this policy and the procedures for the secure destruction of secure data
- Monitoring the purchase and proper maintenance of any equipment used for secure destruction (e.g., software).
- Monitoring Heller's compliance with this policy and applicable state and federal law regarding disposal of secure data

3. Destruction procedures for paper documents include shredding the documents using an industry-acceptable shredder, and disposing of the waste in a secure manner.

4. Destruction procedures for electronic media and other media: An employee disposing of electronic media, or non-paper and non-electronic media containing personal information shall do so by one of the following methods:
    a. Computers, servers, and portable digital assistant ('PDA') devices:
        i. When secure data is no longer covered by a data use agreement, all copies of those data shall be destroyed using software programs designated by the Data Security Committee or specified by the Funder. For example, CMS requires a triple swipe method for safe deletion of sensitive material. Heller operationalizes this using a program called File Shredder that can be downloaded at the following address: http://www.fileshredder.org/.
        ii. The Heller standard is a data destruction method that uses a minimum of a triple swipe technique, such as File Shredder that can be downloaded at the following address: http://www.fileshredder.org/.
        iii. If personal information cannot be securely erased from the device, the hard drives or other components containing the personal information shall be securely destroyed. In this situation, personal information shall be physically removed and destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.
    b. Zip drives, floppy disks, etc. and optical storage media:
        i. Prior to disposal, all electronic data storage media such as external hard drives, zip drives, tape drives, floppy disks, memory cards, memory sticks, USB flash drives, or other electronic storage media containing personal information shall have the data contained in the item destroyed by either wiping the media with a degaussing magnet, by using File Shredder, or by physically destroying the media through shredding or similar physical destruction.
        ii. CDs, DVDs and other optical storage media must be disposed of by physical destruction of the media, such as by shredding.

5. Reporting data destruction: In order to monitor the status of secure data, Principal investigators or others responsible for the propagation of secure data must notify the DUA Database Administrator, in writing, when data destruction is complete, using the Heller Certificate of Disposition (COD) or the funders' own COD. Principal investigators must also notify the originator of the data (e.g., CMS) when required to do so by the data use agreement. Please find a Heller Certificate of Disposition for Data (Form 5) in Section 6 Forms of this document.

6. Reports of violations: Employees should immediately notify the Heller Information Security Committee, the PI, the Brandeis IRB, and the Heller Dean of any violation of this policy, or of any concerns they may have regarding the secure disposal or destruction of secure data.