UNIVERSITY OF NOTRE DAME

Information Handling Standard for HIPAA Data
Version 1.0

1. Introduction

This standard establishes the University practices for HIPAA data handled, stored, sent, received, or accepted by the University of Notre Dame and in compliance with 45 CFR 160 and 164. All University use of HIPAA data on campus must be done as part of an approved business process by individuals designated in the Covered Entity or with a Business Associate Agreement and as mandated by the HIPAA Oversight Committee.

2. Standard

1. Paper Records
   1.1. Papers and forms containing HIPAA Data ("paper records") must be kept in a physically secured location such as a locked cabinet and/or office in accordance with their records retention schedule.
   1.2. When paper records are destroyed, the individual destroying the records must use Secure Shred.

2. Electronic Records
   2.1. Electronic use or storage of HIPAA Data ("electronic records") must be approved by the HIPAA Oversight Committee and Information Governance Committee.
   2.2. Electronic records must be stored in CORPFS, or another file system or application approved by the Information Governance Committee for storage of highly sensitive data. Data must be encrypted. Unencrypted local drives may not be used for storage of electronic records.
   2.3. When electronic records are destroyed, the individual destroying the records must use Secure Erase.
   2.4. An accurate inventory of media containing electronic records must be maintained at all times.

3. Transmission
   3.1. Electronic transmission of HIPAA Data must be done in an encrypted form, using encryption methods on the University's list of approved encryption methods.
   3.2. File transfer must include only the encrypted file. Passwords must be transferred under separate cover.
   3.3. Transmission must be done through a secure website to a Covered Entity or to an entity covered by a Business Associate Agreement.

4. Removable Media
   4.1. HIPAA Data stored on removable media such as USB removable drives ("thumb drives"), CDs, or DVDs must be:
      4.1.1. stored in an encrypted form as individual files OR be stored on encrypted media; and
      4.1.2. must use password protection; and

4.1.3. must be physically stored in a locked storage location with minimal access when not in immediate use by an approved user.

4.2. An accurate inventory of data stored on removable media must be maintained at all times.

5. Retention schedule

5.1. HIPAA Data collected and stored as part of an Approved Business Process must have a designated retention schedule in compliance with the University records retention schedules found at http://archives.nd.edu/records.

3. Definitions

Approved Business Process	An Approved Business Process must be approved by the Information Governance Committee and must have a business process document on file, and appropriate security and access controls in place for the process.
Business Associate	Third parties who perform functions for a Covered Entity involving the use or disclosure of individually identifiable health information and who have a written agreement or contract with a Covered Entity to protect the health information.
Covered Entity	Organization or group that provides or pays the cost of medical care including health plans, healthcare providers and healthcare clearinghouses.
HIPAA Data	• Health Information, including demographic information • Relates to an individual's physical or mental health or the provision of or payment for health care • Identifies the individual • Transmitted or maintained in any form or medium by a Covered Entity or its Business Associate
Secure Erase	Electronically shredded using a program such as Eraser, DBAN, Identity Finder's shred capability or the MacOS secure file delete facility.
Secure Shred	Shredded using a crosscut shredder, or by placing the document in one of the campus provided secure shred bins.
University Network	Networks that Notre Dame owns and maintains