
Retention and Destruction/Disposal of Regulated Information

POLICY CONTENTS

- Scope
- Policy Statement
- Reason for Policy
- Procedures
- Definitions
- Additional Contacts
- Forms
- Related Information
- History

Scope

This policy applies to all university personnel and entities that have access to and electronically store regulated data and/or collect, store and use personal information.

Policy Statement

Retention

It is the policy of the University of Nebraska Omaha (UNO) and its affiliated entities to ensure the privacy and security of proprietary and regulated information in the maintenance, retention, and eventual destruction/disposal of such media. All destruction/disposal of regulated information media will be performed in accordance with federal and state law and pursuant to the UNO Record Retention Schedule. Records that have satisfied the period of retention will be destroyed or disposed in an appropriate manner.

The retention schedule for destruction or disposal shall be suspended for records involved in any open investigation, audit, or litigation. Individuals who know or suspect that confidentiality has been breached by another person or persons have a responsibility to report the breach to the respective supervisor or administrator or to the Human Resources Department. Employees must not confront the individual under suspicion or initiate investigations on their own since such actions could

compromise any ensuing investigation. All individuals are to cooperate fully with those performing an investigation pursuant to this policy.

Disposal/Destruction

Department administration shall determine what information entrusted to their department is private and/or confidential (regulated) and shall communicate methods of protecting that information through the destruction/disposal process to appropriate persons associated with their department.

All paper waste that may contain regulated data must be shredded. Environmental Services (EVS) is responsible for the security, transport, and storage of confidential paper waste from internal customer locations. EVS will secure the confidential waste in locked containers provided by the UNO Recycling Center. The UNO Recycling Center will be responsible for disposing the recycled material in a secure manner and ensuring that all documentation necessary for demonstrating compliance with regulations is maintained. Failure to appropriately dispose or destroy regulated information may result in sanctions, civil or criminal prosecution and penalties, scholastic or employment corrective action which could lead to dismissal, or, as it relates to healthcare professionals or others outside of UNO, suspension or revocation of all access privileges.

All electronic media that contains regulated data must be recycled through the Mailroom or the Information Security Office. The Information Security Office maintains records of destruction for the period outlined in the UNO Record Retention Schedule.

Reason for Policy

Retention and subsequent destruction/disposal of proprietary and Protected Health Information (PHI) are governed by federal and state regulations and university policies and procedures. These regulations and guidelines include, but may not be limited to:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- NU Executive Memorandum 27, HIPAA Compliance Policy
- Board of Regents Bylaws
- Board of Regents Policies
- Information Security Policy
- Institutional Review Board Guidelines, Retention of Research Records for Non-Exempt Research
- Information Technology Services Procedures
- NU Record Retention Schedule

Procedures

This policy is enforced by the Executive Regulated Data Authorization Committee. Failure to comply with this policy may result in disciplinary actions.

Definitions

Information: Data presented in readily comprehensible form. (Whether a specific message is informative or not depends in part on the subjective perceptions of the person who receives it.) Information may be stored or transmitted via electronic media, on paper or other tangible media, or

be known by individuals or groups. Information generated in the course of university operations is a valuable asset of the university and belongs to the university.

Proprietary Information: Information regarding business practices, including but not limited to, financial statements, contracts, business plans, research data, employee records and student records:

- **Employee records** refers to all information, records and documents pertaining to any person who is an applicant or nominee for any university personnel position described in the Board of Regents Bylaws §3.1, regardless of whether any such person is ever actually employed by the university, and all information, records and documents pertaining to any person employed by the university.
- **Student education records** means any information recorded in any way which directly relates to a student and is maintained by or on behalf of UNO (education agency/institution).

Student education record does not include a (i) sole possession record, (ii) law enforcement record, (iii) employee record of a person other than a student who is employed by UNO by virtue of his or her status as a student at UNO, (iv) alumni record and (v) medical record that is part of the common medical record shared by UNO, The Nebraska Medical Center, UMA and UDA. (NOTE: The HIPAA privacy regulation does not apply to education records covered by FERPA.)

Protected Health Information (PHI): Individually-identifiable health information. Health information means any information, whether oral or recorded in any medium, that:

- Is created or received by UNO; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Records containing PHI, in any form, are the property of UNO. The PHI contained in the record is the property of the individual who is the subject of the record.

Cardholder Data: Full magnetic stripe or the Primary Account Number (PAN) plus any of the following:

- Cardholder name
- Expiration date
- Service code (CVV or equivalent)

Cardholder Data Environment: Area of the computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.

Forms

[Regulated Data Authorization Form](#)

Related Information

[NU Executive Memorandum 16](#)

[NU Executive Memorandum 26](#)

[NU Executive Memorandum 27](#)

[UNO Student Records Policy](#)

[State of Nebraska Consumer Notification of Data Security Breach Act of 2006](#)

[Payment Card Industry Data Security Standards \(PCI-DSS\)](#)

[UNO Regulated Data Security Policy](#)

[NU Record Retention Schedule](#)

History

This policy is an update to the Retention and Destruction/Disposal of Private and Confidential Information Policy that was previously updated in 2015.

The University of Nebraska does not discriminate based on race, color, ethnicity, national origin, sex, pregnancy, sexual orientation, gender identity, religion, disability, age, genetic information, veteran status, marital status, and/or political affiliation in its programs, activities, or employment.