



UNIVERSITY POLICY

SUBJECT:	INFORMATION SERVICES AND TECHNOLOGY	TITLE:	PROTECTION AND AUTHENTICATION OF ELECTRONICALLY COMMUNICATED CONFIDENTIAL OR SENSITIVE INFORMATION		
CATEGORY: Check One	Board of Trustees <input type="checkbox"/>	Presidential <input checked="" type="checkbox"/>	Functional <input type="checkbox"/>	School/Unit <input type="checkbox"/>	
Responsible Executive:	Vice President for Information Services and Technology		Responsible Office:	Information Services and Technology	
CODING:	00-01-95-15:00	ADOPTED:	02/04/03	AMENDED:	08/17/10
			LAST REVIEWED: 08/17/10		

I. PURPOSE

To ensure UMDNJ’s compliance with regulatory and statutory requirements regarding data security, and to protect the University’s data and information from unauthorized access and mitigate the risks of loss or theft.

II. ACCOUNTABILITY

Under the President, the Senior Vice President for Administration and the Executive Vice President for Academic and Clinical Affairs shall ensure compliance with this policy. The Deans, Vice Presidents and Presidents/CEOs of the Healthcare Units shall implement the policy in a uniform and consistent manner in accordance with the principles, procedures and standards set forth herein.

III. DEFINITIONS

- A. Confidential or sensitive information is information protected from general access by University policy, State or Federal regulations. Examples include patient, student or employee health records, personnel records, financial data and communications pertaining to such information.
- B. Protection means the safeguarding of information against unauthorized access either in transport or at the end points of the communication system.
- C. Authentication is the identification of the individual communicating the information.
- D. Cryptography is a method used to disguise sensitive information (whether stored or transmitted) from unauthorized parties. UMDNJ uses various encryption technologies to secure confidential information that is stored or transmitted.

IV. REFERENCES

- A. Code of Federal Regulations, Title 45, Part 164, Security and Privacy/(HIPAA)
- B. Rights & Responsibilities for the Use of University-
Accessed Electronic Information Systems [00-01-10-40:00](#)
- C. Information Management [00-01-10-30:00](#)

- D. Facsimile (Fax) Machine Transmittal of Confidential, Sensitive or Protect Health Information [00-01-15-35:00](#)
- E. Family Educational Rights and Privacy Act [00-01-25-05:00](#)
- F. Patient Confidentiality and Health Information [00-01-40-60:00](#)

V. APPLICABILITY

This policy applies to confidential and/or private information as defined by regulation or statutes, University policies (particularly University policy, Information Management, 00-01-10-30:00 section D.2), or data custodians.

VI. POLICY

A. Requirements:

1. Confidential or private information must be identified (as defined in the Information Management policy) by the data custodian and secured appropriately when being transported electronically.
2. Only UMDNJ-managed systems and equipment can be used to transport University information (regardless of classification), unless exempted by University policy, regulatory or statutory requirements, or contractual obligations.
3. When exchanging University information with third parties (contractual parties, industry peers, regulators, etc.) data custodians must ensure that appropriate controls are used to ensure the confidentiality, integrity, and availability of the information.
4. Confidential or private information must be protected according to University standards, regulatory or statutory requirements, or contractual obligations. When required, encryption must be used to securely transport information.
5. All members of the University community are required to use technologies provided and maintained by the University for the protection of all information governed by this policy.

B. Responsibilities:

1. Information Services and Technology (IST) shall develop, implement, and maintain the technology and operational policies and standards necessary to meet the security requirements of the University, its partners, and regulatory and statutory agencies.
2. VPs and Deans will assign a data steward (or stewards) to its information assets, as required by the Information Management policy. They shall implement and enforce the policies and standards governing their information assets and train their staff to follow the University's requirements. They will report loss, theft, or unauthorized disclosures of confidential or private information to Compliance and Legal.
3. Data Stewards shall enforce the policies and standards governing their assigned information assets, as required in the Information Management policy. They will report loss, theft, or unauthorized disclosures of confidential or private information to their VP and/or Dean, or to Compliance and Legal.

VII. NON-COMPLIANCE AND SANCTIONS:

The failure to employ and use the University's supported technology for the protection of confidential or sensitive information may place the offender and the University at significant legal and financial risk. Violation of this policy including the exposure of sensitive information or the theft or misuse of digital credentials may result in denial or removal of access privileges to the University's electronic systems; disciplinary action under applicable University policies; civil litigation; and/or civil or criminal prosecution under applicable state and federal statutes.

By Direction of the President:

Signature on file

Vice President for Information Services and Technology