



UNIVERSITY POLICY

SUBJECT: INFORMATION SERVICES AND TECHNOLOGY **TITLE:** PROTECTION AND AUTHENTICATION OF ELECTRONICALLY COMMUNICATED CONFIDENTIAL OR SENSITIVE INFORMATION

CODING: 00-01-95-15:00 **ADOPTED:** 02/04/03 **AMENDED:** 02/04/03

I. PURPOSE

To ensure UMDNJ's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Standards for Security and Privacy and establish the principles and set the overall policy framework by which confidential or sensitive information can be communicated through the University's networked systems.

II. ACCOUNTABILITY

Under the President, the Senior Vice President for Administration and Finance and the Senior Vice President for Academic 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. APPLICABILITY

This policy shall apply to electronically communicated confidential, sensitive or health information protected from general access by State and Federal regulations or University policy. Confidential and sensitive information includes patient, student, employee health, personnel records, financial data and communications pertaining to such. Health information that is generated during provisions of health care to patients in any of the University's patient care units, patient care centers or faculty practices as well as Human Subjects research under the auspices of the University or by any of its agents in all UMDNJ Schools, Units, Departments and University owned or operated facilities.

IV. 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. Public Key Infrastructure is a technology for enabling the secure transport of information accessible only to specific individual(s) and establishing non-repudiated identity of the sender.

V. REFERENCES

- A. Code of Federal Regulations, Title 45, Part 164, Security and Privacy/(HIPAA)
- B. UMDNJ Standard Certificate Policy
- C. UMDNJ Key Recovery Policy and Procedures
- D. UMDNJ Public Key Infrastructure (PKI) User Responsibilities Agreement

Documents B-D can be accessed at the following website:
<http://www.umdj.edu/istweb/pki/repository>.

The following policies provide additional and related information:

- E. Rights & Responsibilities for the Use of University-
Accessed Electronic Information Systems [00-01-10-40:00](#)
- F. Information Management [00-01-10-30:00](#)
- G. Patient Confidentiality and Health Information [00-01-40-60:00](#)
- H. Family Educational Rights and Privacy Act [00-01-25-05:00](#)
- I. Facsimile (Fax) Machine Transmittal of Confidential,
Sensitive or Protect Health Information [00-01-15-35:00](#)

A. Requirements:

- 1. Confidential or sensitive information may be communicated electronically only through systems capable of preventing access by anyone other than the intended recipient(s) and establishing the non-repudiated identity of the sender.
- 2. The University has elected to use a technology known as Public Key Infrastructure (PKI) to assure the protection and authentication of electronically communicated information.
- 3. 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) will establish and maintain the technical apparatus and procedures necessary to support PKI certificates for the University. This will include certificate issuance, training and installation or configuration of software required by the end user.
- 2. Employees and students of the University will obtain PKI certificates from the University and employ such certificates in conjunction with supported communication software whenever communicating information is classified as confidential or sensitive.
- 3. IST will establish a Key Recovery Review Committee to provide assistance and advice with regard to the recovery of documents in situations where the key used for encryption and or signature has been lost or revoked, perhaps as the result of employee or student termination.

4. Application for PKI certificates may only be made in person at locations designated by IST.
5. As a condition of issuance, the certificate holder must read and sign the UMDNJ PKI User Responsibilities Agreement.
6. The University considers its PKI certificates as providing positive identification of the holder. Sharing PKI certificates is prohibited.

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 theft of a digital signature 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:

Vice President for Information Services and Technology