UNIVERSITY OF MAINE SYSTEM
HIPAA POLICY #44
SECURITY OF PHI – TECHNICAL SAFEGUARDS

I.   Access Control

The Covered Component shall implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

> A. Unique user identification (Required). The Covered Component shall assign a unique name and/or number for identifying and tracking user identity.
> B. Emergency access procedure (Required). The Covered Component shall establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.
> C. Automatic logoff (Addressable). The Covered Component shall implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
> D. Encryption and decryption (Addressable). The Covered Component shall implement a mechanism to encrypt and decrypt electronic PHI.

II.   Audit Controls

The Covered Component shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

III.   Integrity

The Covered Component shall implement policies and procedures to protect electronic PHI from improper alteration or destruction.

> A. Mechanism to authenticate electronic PHI (Addressable). The Covered Component shall implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

IV.   Person or Entity Authentication

The Covered Component shall implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

V.   Transmission Security

The Covered Component shall implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

> A. Integrity controls (Addressable). The Covered Component shall implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.
> B. Encryption (Addressable). The Covered Component shall implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

Revised 02/09/2010