Subject: Portable Computing Device Security Policy
Policy #: Information Security-P#9.8.1
Coverage: OUHSC
Version: 1.0
Regulation: HIPAA, FERPA, GLB, State of Oklahoma OSF
Approved: 11/16/05
Effective: 11/16/05
Revised/Reviewed: 11/18/2014

Purpose: The portability offered by PCDs and their media increases the risk of theft or loss. In addition, the threat of malicious code infection and network or wireless data interception (sniffing) for these devices is increasing. These risks may result in costs associated with replacement of the data and physical device, lost productivity, legal liability, and loss of reputation or negative publicity.

The purpose of this policy is to establish safeguards for the use of PCDs and their media to protect information from unauthorized disclosure, use, modification, and loss.

Policy: All Portable Computing Devices (PCDs), irrespective of device ownership, that are used in conjunction with any computer, data, or network device owned or managed by OU must follow OU policies and standards for the secure use of PCDs. This includes personal devices that access OU email systems. See Standards for Portable Computing Device Security.

Scope/Applicability: This policy is applicable to all workforce members who use PCDs in conjunction with any OU computer, data, or network.

Regulatory Reference:
HIPAA 45 CFR 164.310(b) [HIPAA Security rule: workstation use]
FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act]
ISO 17799: 9.8 Mobile computing

Definitions: See the Information Security Policy Definitions document for definitions

Responsible Department: Information Technology will maintain PDC standards for safe computing.

Enforcement/Audit: The University’s Internal Auditing department will periodically assess departmental compliance.

Related Policies: Standards for Portable Computing Device Security, Data Classification Policy, PHI Server Consolidation Policy, Data Disposal and Reuse Policy, Antivirus Policy, Data Protection Standard, Desktop Standards

Procedures: Each department that maintains information systems and electronic media is responsible for developing procedures to comply with this policy.

Renewal/Review: This policy is to be reviewed and updated as needed by IT Information Security Services.