

**Procedure Title: Confidentiality of Faculty, Staff and College Business Information (HIPAA)**

**Procedure Number: 03-2003-0004**

**Board Policy Reference: IV.A. General Executive Direction**

**NWCCU Standard:**

---

**Accountable Administrator:** Chief Human Resources Officer

**Position responsible for updating:** Chief Human Resources Officer

**Original Date:** August 2003

**Date Approved by Cabinet:**

**Authorizing Signature:** *Signed original on file*

**Dated:** 12-16-03

**Date Posted on Web:** 07-15-09

**Revised:** 07-09

**Reviewed:** 07-13

---

**Purpose/Principle/Definitions:**

It is the legal and ethical responsibility of all BMCC faculty, staff and student employees, and volunteers to use personal and confidential health, employee and College business information (referred to here collectively as “confidential information”) in accordance with the state and federal laws and college policy, and to preserve and protect the privacy rights of the subject of the information as they perform their college duties.

Laws controlling the privacy of, access to and maintenance of confidential information include, but are not limited to, the federal Health Insurance Portability and Accountability Act (HIPAA). This and other laws apply whether the information is held in electronic or any other form, and whether the information is used or disclosed orally or in writing.

BMCC policies that control the way confidential information may be used include, but are not limited to BMCC Personnel Policies, applicable bargaining agreement provisions, and as summarized below.

Confidential information includes information that identifies or describes an individual and the disclosure of which would constitute an unwarranted invasion of personal privacy. Examples of confidential employee and college business information include home addresses and telephone number; medical information; birth date; citizenship; social security number; spouse/partner/relative’s names; income tax withholding data and performance evaluations.

The term “medical information” includes the following: medical and psychiatric records, including paper printouts, photos, videotapes, diagnostic reports, insurance information whether stored externally or on campus; electronically stored or transmitted medical information; verbal information provided by or about an employee; peer review/risk management information and activities; or other information the disclosure of which would constitute an unwarranted invasion of privacy.