



# Confidentiality and Privacy Under HIPAA

Effective: April 14, 2003

Last Review: July 2, 2020

**SUBJECT:** Confidentiality and Privacy Policy under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

**SCOPE:** All Employees

**PURPOSE:** To Establish the Responsibility of Employees to Protect the Confidentiality of Confidential Information to Which They Have Access

Policy Statement: All VSU employees must hold confidential information used or obtained in the course of their duties in confidence. All protected health information (PHI) must be treated as confidential in accordance with professional ethics, accreditation standards, and legal requirements. All employees with access to confidential information, including patients' medical records information, employment information and/or information systems must read and sign the VSU Confidentiality and Security Access Agreement, which will be kept on file and updated annually.

## Definitions:

Confidential Information: all records, files, reports, protocols, policies, manuals, databases, processes, procedures, computer systems, materials and other information pertaining to the operations of VSU, as well as all individually identifiable health information pertaining to patients of VSU. Confidential information includes, but is not limited to, past, present or future information about a patient's condition or treatment, aggregate clinical data, employee records, processes, marketing plans or techniques, product or service plans, strategies, forecasts, customer/patient lists, supplier lists, discoveries, ideas and financial information. Confidential information may be obtained by hearing it, seeing it, viewing a medical record or accessing a hospital computer system, and it may be in any form including, but not limited to, paper, a computer screen, electronic media, a recording device, etc.

Need-to-know: that which is necessary for one to adequately perform one's specific job responsibilities at or for VSU.

Associates: includes, but is not limited to, all residents, physicians, volunteers, affiliated students, vendors, contractors and any external agencies that have access to confidential information about VSU or its patients.

Maintain a list for six years of Protected Health Information for each patient and those made pursuant to an authorization as required by HIPAA rules.



# Confidentiality and Privacy Under HIPAA

## Proprietary Information

It is the policy of VSU to respect the proprietary rights of the companies that develop and support the computer software we use. All VSU employees who use a personal computer system are required to comply with license agreements associated with the computer software products used. Personal computer systems may not be used for any purpose that violates the law. It is against VSU policy to make illegal copies, download or transmit information or software in violation of copyright laws. No software may be installed on any computer system without prior authorization from Information Services.

## Monitoring Access to Patient and Other Confidential Data

Information Services is responsible for data security and shall audit the access to enterprise-wide systems and data. This includes, but is not limited to, access to Network, Email, Internet, PRISM, Medipac, Human Resources, Accounts Payable, Payroll, General Ledger and TESS.

## Protecting Confidential Information

Employees of VSU have a responsibility to protect confidential information and adhere to the standards set forth in the Notice of Health Information Privacy Practices. Therefore, employees may not use or disclose confidential information except in accordance with the law and applicable VSU policies and procedures. Employees shall not disclose information in any form (whether verbal, written, electronic, by fax, etc.) without authorization.

### Verbal Communication

While on duty at VSU, confidential information shall not be discussed where others may hear the conversation, such as in hallways, on elevators, in the cafeteria, etc. Dictation of patient information should occur in locations where others cannot overhear. While off duty, employees shall not discuss any confidential information.

### Written Communication

Confidential papers, reports and computer printouts should be kept in a secure place. Confidential documents should not be left unattended or where they may be viewed by others who do not have a need to know. Confidential documents should be retrieved as soon as possible from copiers, mailboxes, conference room tables and other publicly accessible locations. When no longer needed, confidential documents should be deposited in the document destruction bins. Confidential documents shall not be sent or taken outside of VSU except in accordance with applicable VSU policies and procedures.

### Electronic Communication

All confidential information residing within computers, networks, servers, software applications, electronic mail, diskettes and any other storage media is the sole property of VSU. Confidential information should not be sent or taken outside the organization or disclosed to anyone who does not have a need-to-know, except in accordance with applicable VSU policies and procedures.



# Confidentiality and Privacy Under HIPAA

Computer monitors should be positioned so that others cannot easily view the information. A computer user must log out of any computer session opened under his or her user name and password prior to leaving any computer or terminal unattended. Users should always be aware of anyone around them who does not have a need to know so that confidential information is not exposed.

## Faxed Information

All employees shall take precautions to protect confidential information when using fax machines to transmit or receive documents, as specified in more detail in the VSU Fax Confidentiality and Security Policy. All fax machines shall be located in secure areas away from public access. When sending a fax, be absolutely sure that the correct number is dialed and that a cover sheet is always used. The cover sheet should contain the sender's name, the sender's contact number, the receiver's name, the receiver's fax number, the number of pages and the VSU standard confidentiality statement. When receiving a fax, immediately remove the fax transmission from the fax machine and deliver it to the intended recipient. Destroy or place in a document destruction bin any confidential information received in error and immediately inform the sender.

## Confidentiality Violations to be Avoided

Carelessness - An employee or associate unintentionally or carelessly accesses, reviews or reveals confidential information to him/herself or others without a legitimate need-to-know. Examples include, but are not limited to: an employee or associate discussing confidential information in a public area; an employee or associate leaving a copy of confidential information unsecured; an employee or associate leaving a computer on which confidential information is displayed unattended or unsecured.

Curiosity or Concern (no personal gain) - An employee or associate intentionally accesses, reviews or discusses confidential information for purposes other than the care of the patient or authorized purposes, but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee or associate looking up a birth date or an address of a friend or relative; an employee or associate accessing and reviewing a patient's record out of concern or curiosity.

Personal Gain or Malice - An employee or associate accesses, reviews or discusses confidential information for personal gain or malicious intent. Examples include, but are not limited to: an employee or associate reviewing, accessing or communicating confidential information for use in a personal relationship; an employee or associate compiling a mailing list for personal use or to be sold; an employee or associate using confidential information to hurt or harm others.

## Consequences of Confidentiality Violations

The consequences of violating the confidentiality of patient information, employee information, business information, financial information and other confidential information relating to VSU may result in discipline up to and including immediate termination.

Violation of confidentiality policies may also lead to civil and criminal liability.



# Confidentiality and Privacy Under HIPAA

## Affected Stakeholders

Indicate all entities and persons within the university affected by this policy:

- Alumni       Graduate Students       Undergraduate Students  
 Staff       Faculty       Student Employees  
 Visitors       Vendors/Contractors       Other: \_\_\_\_\_

## Policy Attributes

<i>Responsible Office(s)</i>	Information Technology, 1410 N. Oak St., 229-245-4357, itvsu@valdosta.edu
<i>Approving Officer or Body</i>	President, President's Office, West Hall Suite 1004, 229-333-5952, president@valdosta.edu
<i>Date Approved</i>	04/14/2003
<i>Last Review Date</i>	07/02/2020
<i>Next Review Date</i>	07/02/2022