VUMC CONFIDENTIALITY AND ACCESS POLICY

As a member of the Vanderbilt community you may have access to "confidential information." The purpose of this agreement is to help you understand your duty regarding confidential information as described in this policy. Members of the Vanderbilt community include but are not limited to physicians, faculty, staff, volunteers, and students and vendors.

Measures must be taken so that all information captured, maintained, or utilized by VUMC and any of its off-site subsidiaries and affiliates can only be accessed by authorized users. VUMC has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information and all other types of confidential information. Patient information is confidential information regardless of how it is obtained, stored, utilized, or disclosed.

As a member of the Vanderbilt community you are required to conduct yourself in strict conformance to all applicable laws and Vanderbilt University and VUMC policies governing confidential information. Your principal obligations in this area are explained below. You are required to read and to abide by these duties. The violation of any of these duties will subject you to disciplinary action, which might include, but is not limited to, termination of employment and/or ability to do business with VU or VUMC, and may subject you to legal liability as well.

As a member of the Vanderbilt community, you will likely have access to and use confidential information in any or all of the following categories:

- Patient information (such as charts and other paper and electronic records, demographic information, conversations, admission/discharge dates, names of attending physicians, patient financial information, etc.);
- Information pertaining to members of the Vanderbilt community (such as salaries, employment records, student records, disciplinary actions, etc.);
- Vanderbilt University and VUMC information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary information including computer programs, source code, proprietary technology, etc.); and
- Third-party information (such as insurance, business contracts, vendor proprietary information source code, proprietary technology, etc.).

Vanderbilt University Medical Center

VUMC CONFIDENTIALITY AGREEMENT

As a condition of and in consideration of my use, access, and/or disclosure of confidential information,

I, _____ understand and agree to the security requirements outlined in this Agreement. **I understand that these security requirements and my responsibility to protect confidential information also apply to when I'm working from home or off-campus.**

1. I will access, use, and disclose confidential information only as necessary to perform my job functions. This means, among other things, that:

   a) I will only access, use, and disclose confidential information which I have authorization to access, use, and disclose which is required to do my job;

   b) I will not in any way access, use, divulge, copy, release, sell, loan, review, alter, or destroy any confidential information except as properly and clearly authorized within the scope of my job and as in accordance with all applicable Vanderbilt policies and procedures and with all applicable laws;

   c) I will report to my supervisor or to the appropriate office any individual's or entity's activities that I suspect may compromise the confidentiality of confidential information as prescribed in OP 10-17 "Confidentiality of Protected Patient Information".

(Section 2 only applies if you have been granted electronic access to VU/VUMC systems, <u>including email</u>.)

2. Because all of my User ID/Passwords are the equivalent of my signature and because I am the only person authorized to use them, I agree to the following:

   a. I will safeguard and not disclose my passwords, access codes or any other authorizations I have that allow me to access confidential information to anyone <u>including my manager, supervisor, or LAN Manager.</u>

   b. I will not request access to or use any other person's passwords or access codes.

   c. I accept responsibility for all activities undertaken using my passwords, access code and other authorizations.

   d. It is my responsibility to log out of the system to which I'm logged on. I will not under any circumstances leave unattended a computer to which I have logged on without first either locking it or logging off the workstation.

   e. If I have reason to believe that the confidentiality of my password has been compromised, I will change my password.

   f. I understand that my User ID will be deactivated upon notification to Information Management that I am no longer employed by or in a business contract with VUMC, have no medical staff privileges at a VUMC institution, am not enrolled as a student in a healthcare profession, or when my job duties no longer require access to the computerized systems.

   g. I understand that the Department of Information Management has the right to conduct and maintain an audit trail of all accesses to patient information, including the machine name, user, date, and data

accessed and that VUMC may conduct a review of my system activity at anytime and without notice to monitor appropriate use.

h. I understand and accept that I have no individual rights to or ownership interests in any confidential information referred to in this agreement and that therefore VU or VUMC may at any time revoke my passwords or access codes.

3. All individuals who take work home with them must follow Vanderbilt's Security Guidelines for Remote Access.

4. I understand that it is my responsibility to be aware of VU Human Resource policies including HR-025 "Electronic Communications Policy", VUMC Operation Policies, and other policies that specifically address the handling of confidential information and misconduct that warrants immediate discharge.

5. I understand that in addition to protecting confidentiality I am also required to be aware of the VU Computer Privileges and Responsibilities policy and to abide by all of its requirements regarding the appropriate use of VU and VUMC computer systems. I understand that inappropriate use of VU and VUMC computer systems may result in disciplinary action.

6. I understand that any fraudulent application, violation of confidentiality or any violation of the above provisions may result in disciplinary action, including loss of system and information access privileges, as well as other appropriate disciplinary measures up to and including termination of employment and/or affiliation with VU and VUMC.

My signature below indicates that I have read, accept, and agree to abide by all of the terms and conditions of this Agreement and agree to be bound by it.

Signature: _____ Date: _____

Printed Name: _____

Job Title: _____ Department/School: _____

Summary Points

- **I will access, use, and disclose confidential information only as authorized and needed to perform my job duties for VU and VUMC.**
- **I am responsible for all actions taken using my User-ID/Passwords and other authentication devices. I agree not to allow others to use my User-ID/Passwords. I agree not to attempt to use any authentication devices belonging to others.**
- **I will use VU computer systems only as outlined in the VU Computer Privileges and Responsibilities policy.**
- **Any violation of confidentiality as outlined in this agreement will result in disciplinary action, which may include, but is not limited to, loss of system access privileges, loss of clinical privileges, suspension, termination, and/or loss of ability to do business with VUMC.**

References:
HR-025, "Electronic Communications" – www.vanderbilt.edu/HRS/hrs.htm
VU Computer Privileges and Responsibilities – www.vanderbilt.edu/aup.html
VUMC Operations Policies – http://vumcpolicies.mc.vanderbilt.edu/E-manual/Hpolicy.nsf
Security Guidelines for Remote Access – www.mc.vanderbilt.edu/security

Last Revised 12/01/03