CONFIDENTIALITY AGREEMENT REGARDING ACCESS TO PATIENT INFORMATION

This Confidentiality Contract ("Agreement") is entered into by and between Vanderbilt University by and through its Vanderbilt University Medical Center, a not for profit Tennessee Corporation ("VUMC") and ____________________________, ("Company"). The purpose of this Contract is to ensure that access by non-VUMC staff or faculty to VUMC patient information is consistent with VUMC policies and in compliance with all applicable state and federal laws, and accreditation standards. Company employees who require access to VUMC information systems containing patient information to perform their patient care duties and/or administrative duties must obtain prior authorization for such access and protect the confidentiality and security of VUMC patient information as described below.

TERMS AND CONDITIONS:

Company has requested that VUMC grant access to VUMC patient information by certain of Company’s employees listed in Exhibit A for the purpose of (please check all that apply):

- Patient care/continuing care
- Benefits/utilization/quality review
- Billing
- Other (specify) ________________________________

1. Company agrees that it is an Extended Community Member as defined in the VUMC policy on Access to Confidential Information attached hereto as Exhibit B and agrees to maintain the confidentiality of patient information in accordance with the policy and the VUMC Confidentiality Agreement (attached as Exhibit C), as they may be amended from time to time.

2. Company agrees to review the Vanderbilt policies related to confidentiality and computer access privileges and responsibilities, attached hereto as Exhibit B, Exhibit C, and Exhibit D, and applicable state and federal laws with Company’s staff and representatives of Company and instruct them as follows:
   - They are to access patient information only as necessary to carry out the responsibilities of their employment.
   - They are to maintain the confidentiality of patient information in accordance with the VUMC Confidentiality Agreement.
   - Violation of patient confidentiality may subject the employee to corrective action up to and including termination of employment and/or suspension and loss of privileges to access VUMC Confidential Information.

3. Company agrees to obtain from each of its employees who uses or has access to VUMC systems and patient information a signed VUMC Confidentiality Agreement (Exhibit C) stating that he or she has been informed and understands the VUMC Confidentiality Agreement and will comply with such Agreement. Company will provide that signed Confidentiality Agreement to VUMC prior to each individual employee being granted access to VUMC patient information.

4. Company agrees to notify Information Management at the VUMC Help Desk (615-343-4357) immediately upon termination of employment of any staff member or representative who has been granted access to VUMC patient information so that access rights for that individual may be
5. Company agrees to cooperate with and provide reasonable assistance to VUMC when necessary to investigate governmental or other complaints or concerns involving Company employee access, use or disclosure of VUMC patient information. Company agrees that VUMC may, at its sole discretion, revoke the access to patient information of any Company employee at any time. Company understands that access may be revoked in the event of a breach of patient confidentiality by Company or any of Company’s employees or representatives. Company agrees to immediately suspend or terminate further access to information by any Company employee who violates the provisions of the Confidentiality Agreement. In the case of a violation of the Confidentiality Agreement by a Company employee, Company agrees to impose discipline that is at least equivalent to the sanction specified in VUMC’s policy on Sanctions for Privacy and Information Security Violations attached hereto as Exhibit D. VUMC may immediately terminate Company’s access in whole or in part if Company fails to take prompt and appropriate action to address any concern reported to Company by VUMC.

6. Company agrees to adopt policies and procedures with regard to maintaining patient information in a secure manner and properly disposing of any information which is no longer needed and which has been converted to another media, e.g., paper, tape, etc.

7. Company agrees to notify the VUMC Privacy Office of any use or disclosure of VUMC patient information by Company or a Company employee not permitted by this Agreement, any Security Incident involving electronic patient information, and any Breach of Unsecured Protected Health Information as defined in the Health Information Technology Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (“HITECH Act”) within five (5) business days.

7.1. Company shall provide the following information to VUMC within ten (10) business days of discovery of a breach except when despite all reasonable efforts by Company to obtain the information required, circumstances beyond the control of the Company necessitate additional time. Under such circumstances Company shall provide to VUMC the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a breach:

1. the date of the breach;
2. the date of the discovery of the breach;
3. a description of the types of unsecured patient information involved;
4. identification of each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
5. any other details necessary to complete an assessment of the risk of harm to the individual.

7.2. VUMC will be responsible to provide notification to individuals whose unsecured patient information has been disclosed, as well as the Secretary and the media, as required by Sec. 13402 of the HITECH Act, 42 U.S.C.A. § 17932 and Company agrees to pay the actual cost of providing such notification(s).

8. Company agrees that VUMC may audit access to and use of its patient information by Company and its employees or representatives at any time or on an ongoing basis and may ask for and receive copies of the signed Confidentiality Agreement described in paragraph 3, above.

9. Special condition(s) that apply to this Agreement, if any, are described here:

a) Company agrees that all Company employees will use restricted panel access to the electronic medical record maintained by VUMC.
b) Company agrees that each employee granted access will use two-factor authentication via an individually assigned RSA Token to access the VUMC systems and data.

c) Company agrees to reimburse VUMC for the cost of the individual RSA Token for each employee granted access.

10. Notice to the VUMC Privacy Office shall be phoned or mailed via email or U.S. Postal at the following contact:

Vanderbilt University Medical Center
Privacy Office
4560 Trousdale Drive
Suite 101
Nashville, TN 37204-2074
(615) 936-3594
privacy.office@vanderbilt.edu

11. This Agreement shall be effective upon the date fully executed and shall remain in effect for so long as and at any time that any employee or representative of Company needs access to VUMC systems and/or information in order to perform the patient care, continuity of care, and/or administrative review duties described above.

12. In the event of a conflict between the terms of this Agreement and the terms of a Business Associate Agreement between the parties, the terms of the Business Associate Agreement shall govern and control.

Company Name: ____________________________

Signature: _________________________________

Signed By: ________________________________

Title: ________________________________

Date: ________________________________

Vanderbilt University, by and through its Medical Center:

Signature: ________________________________

Signed By: ________________________________

Title: ________________________________

Date: ________________________________
EXHIBIT A

Employees or Representatives of Company
EXHIBIT B

ACCESS TO CONFIDENTIAL INFORMATION

I. Outcome Goal:

To uphold legal, ethical, and operational responsibilities of Vanderbilt University Medical Center (VUMC) to appropriately safeguard VUMC confidential information, including individually identifiable patient information.

II. Policy:

Each individual who needs access to VUMC confidential information is required to comply with VUMC policies and procedures for granting access to its information resources and protecting the information obtained in the course of business.

III. Definitions

A. **Workforce Member:** An individual performing work on behalf of VUMC and under the direct control of VUMC, whether or not the member is employed by VUMC. Examples include: staff; faculty; temporary agency workers; students; contractors; and volunteers.

B. **Extended Community Member:** An individual who is present on VUMC premises or accessing information resources at VUMC for a specific treatment, payment, or health care operation business purpose allowed under the Health Insurance Portability and Accountability Act (HIPAA) such as a third party payer representative, a visitor for a guided tour or observation experience, media or vendor representatives, or other health care providers involved in a patient’s continuum of care.

C. **Company:** A person or company that performs certain functions or activities on behalf of, or for, VUMC that involve the creation, use, or disclosure of VUMC protected health information (PHI).

D. **VUMC Confidential Information:** Includes any and all of the following categories of information in paper, verbal, or electronic form regardless of how it is obtained, stored, utilized, or disclosed:

1. Patient information including demographic, health, and financial information;
2. Information pertaining to members of the VUMC Workforce or Extended Community (such as social security numbers, banking information, salaries, employment records, student records, disciplinary actions, etc.);
3. Vanderbilt University or VUMC information (such as research information, financial and statistical records, academic or research funding, strategic plans, internal reports, memos, contracts, peer review information, communications,
proprietary information including computer programs, source code, proprietary technology, etc.);

4. Third-party information (such as insurance, business contracts, vendor proprietary information or source code, proprietary technology, etc.); and

5. Patient, research, academic program, or other confidential or proprietary information heard or observed by being present on VUMC premises.

E. **Compliance or Research Monitor/Auditor:** is an authorized representative of an external agency, sponsor of academic programs or research, or governmental regulatory authority who may be provided with access to confidential information to monitor for compliance with regulatory or contract obligations.

F. **Key Study Personnel (KSP):** individuals identified in a VUMC IRB-approved protocol as having responsibility for interaction with research participants outside of the individual’s normal clinical duties, including those individuals who are responsible for the design or conduct of the research study.

IV. **Specific Information:**

A. **Access to VUMC Confidential Information by VUMC Workforce Member:** Each VUMC Workforce Member signs the VUMC Confidentiality Agreement as part of the employment process, admission to an educational program, contract negotiation, procurement, or vendor registration process. VUMC includes the terms and conditions of the VUMC Confidentiality Agreement in contracts and other documentation for the purchase of products and services, or for accommodation of any other relationships that involve the sharing of VUMC Confidential Information.

1. Organizational units are responsible for providing information about this requirement to prospective faculty/staff, students, other trainees, volunteers, vendors, and affiliates, and for securing signed Confidentiality Agreements in a timely manner.

2. The current, approved form of the VUMC Confidentiality Agreement is available on the VUMC Privacy Office web site.

3. Signed Confidentiality Agreements are stored in the personnel, vendor, or contract file maintained by the organizational unit manager for a minimum of six (6) years in a manner that allows easy access and retrieval.

B. **Business Associate Access:** Business Associates of VUMC are required to enter into a Business Associate Agreement that satisfies all requirements of HIPAA and VUMC Policies. Contract templates and resource information for Business Associate Agreements are available on the VUMC HIPAA website and questions may be directed to the VUMC Privacy Office.

C. **Access to VUMC Confidential Information by Extended Community Members:**

1. When representatives of a company function as Extended Community Members, the company assists VUMC in safeguarding VUMC Confidential Information by, among other means, causing its representatives to sign the
VUMC Confidentiality Agreement and imposing disciplinary action upon a company representative who does not comply with the terms of the VUMC Confidentiality Agreement. Such assurance from the company is preferably reflected in a written contract between the company and VUMC.

2. Each Extended Community Member agrees to abide by a VUMC approved confidentiality agreement that includes, at a minimum, the following safeguards:

   a. To access VUMC Confidential Information only as necessary to carry out the other party’s responsibilities under the contract;

   b. To safeguard and maintain VUMC Confidential Information in accordance with all applicable VUMC policies and procedures applicable to access or use of its information resources;

   c. To acknowledge that appropriate corrective or disciplinary action will be imposed upon an individual who is disruptive or violates VUMC policies;

   d. To safeguard and not disclose the individual user identification password;

   e. To agree that VUMC may, at it sole discretion, revoke access by any individual or entity to VUMC Confidential Information at any time;

   f. To agree that VUMC may audit access to and use of VUMC Confidential Information by the other party and its employees, agents and representatives as applicable at any time and on an ongoing basis.

3. VUMC employs restricted panels, time-limited access and other mechanisms as available and appropriate to limit access by an Extended Community Member to the minimum information necessary to accomplish the specific purpose served by the Extended Community Member.

D. Compliance or Research Monitor/Auditor Access to VUMC Confidential Information:

1. When a written agreement is entered into between VUMC and an external agency or sponsoring company whose Monitor/Auditors require access to VUMC Confidential Information, VUMC includes a provision in the agreement that obligates the sponsoring agency or company to assist VUMC in safeguarding VUMC Confidential Information by complying with VUMC related policies. Such safeguards include, at a minimum, holding the Monitor/Auditor accountable to abide by confidentiality requirements established by VUMC policy and imposing disciplinary action upon or replacement of a Monitor/Auditor who does not comply with the requirements.
2. Each Monitor/Auditor registers their presence on the VUMC campus at the designated administrative office:
   a. State or Joint Commission Surveyors to the VUMC Accreditation and Standards Department;
   b. Sponsored research clinical monitors to the appropriate Office of Research/Department;
   c. Academic or research funding auditors to the Department of Finance, Academic & Research Enterprise;
   d. Other government or agency representatives who present without prior arrangements – call the VUMC Compliance Office.

3. Each Monitor/Auditor provides valid, government issued photo identification from which sufficient personal identification information is extracted for a VUMC employee to authenticate authorization to access confidential information.

4. A VUMC employee provides each Monitor/Auditor with a copy of the Confidentiality Requirements for Compliance/Research Monitors/Auditors and documents the Monitor/Auditor’s verbal agreement to comply with such requirements.

5. Monitors/Auditors of certain external regulatory or sponsoring agencies or companies (e.g. FDA or industry research sponsors) may be granted access to electronic systems in order to access VUMC Confidential Information utilizing a time-limited access registration process administered through the applicable administrative office designated above in D. 2. The Monitor/Auditor receives a unique user name and access code valid for a defined period of time that allows access to a restricted panel of records pertinent to the authorized purpose of the compliance monitoring activity.

E. Temporary Research Key Study Personnel (KSP) Requiring Access to VUMC Confidential Information:

1. A VUMC Principal Investigator (PI) for an approved research project may designate in accordance with this section an individual, who is not otherwise authorized as a VUMC staff or faculty member to access PHI, to participate as KSP on the research project. The PI is responsible for securing approval by the Institutional Review Board (IRB) for the project application or an amendment that identifies the individual as KSP.

2. The individual is required to have a Vanderbilt email address and computer user identification (VU-net ID) and to complete all research training modules required of other research staff in order to be eligible to serve as KSP on a research project.

3. The individual is required to use the StarBrite research website to initiate the on-line application for access to the electronic medical record system.

4. Any such research KSP is required to sign the VUMC Confidentiality Agreement.
5. VUMC employs restricted panels and time-limited access to provide the temporary KSP with the minimum necessary PHI needed to fulfill the role as KSP on the VUMC IRB-approved project.

F. VUMC Confidentiality Policies, Procedures, and Resources: VUMC facilitates access to its most current confidentiality policies and procedures, templates for agreements, and approved forms on the VUMC Privacy Office website. Contact the VUMC Privacy Office with any questions regarding the selection, use, or revision of a VUMC Confidentiality Agreement, Company Agreement, or other privacy-related form.

V. Web References:


https://mcapps.mc.vanderbilt.edu/E-Manual/Policy.nsf?OpenDatabase

OP 10-40.33 Authorization and Access to Electronic Systems and Applications
OP 10-40.15 Use and Disclosure of Protected Health Information
OP 10-40.02 Access to Patient and Patient Records by External Agencies
OP 10-10.17 Company Agreements

http://hr.vanderbilt.edu/policies/index.htm

HR – 025 Electronic Communications Policy

VUMC HIPAA Website. Retrieved June 26, 2009, from:
http://www.mc.vanderbilt.edu/hipaa

VUMC Privacy Office Website. Retrieved June 26, 2009, from:
http://www.mc.vanderbilt.edu/privacy

Research Support Services Website. Retrieved June 26, 2009, from:
http://www.mc.vanderbilt.edu/root/vumc.php?site=support

Vanderbilte StarBRITE Website. Retrieved June 26, 2009, from:
https://www.mc.vanderbilt.edu/starbrite/research/tempksp.html

www.vanderbilt.edu/aup.html
VI. Endorsement:

Office of Research and Research Support Services – June 2009
Information Privacy and Security Executive Committee – June 2009
Operations Policy Committee – July 2009

VII. Approval:

Kevin Churchwell, MD, Executive Director & CEO, VCH 10/15/09
Colleen Conway-Welch, Dean, School of Medicine 7/20/09
Larry Goldberg, Executive Director & CEO, VUH 7/20/09
C. Wright Pinson, MBA, MD 7/20/09
Deputy Vice Chancellor for Health Affairs
CEO of the Hospitals and Clinics for VUMC

David Posch, CEO, The Vanderbilt Clinic 10/16/09
David S. Raiford, MD 7/21/09
Associate Vice Chancellor for Health Affairs
Senior Associate Dean for Faculty Affairs
EXHIBIT C

Confidentiality Agreement

Vanderbilt University Medical Center (VUMC) has legal and ethical responsibilities to safeguard the privacy of its employees, students, and patients and their families and to protect the confidentiality of protected health information and all other types of confidential information. Members of the Vanderbilt community include but are not limited to:

- **Workforce Member**: an individual performing work on behalf of VUMC and under the direct control of VUMC, whether or not the member is employed by VUMC. Examples include: staff; faculty; temporary agency workers; students; contractors; and volunteers.
- **Extended Community Member**: an individual who is present on VUMC premises or accessing VUMC Confidential Information resources for a specific treatment, payment, or health care operation business purpose allowed under the Health Insurance Portability and Accountability Act (HIPAA) such as a third party payer representative, a visitor for a guided tour or observation experience, media or vendor representatives, or other health care providers involved in a patient's continuum of care.
- **Company**: is a person or company that performs certain functions or activities on behalf of, or for, VUMC that involve the creation, use or disclosure of VUMC protected health information.

As a member of the Vanderbilt community I agree to conduct myself in strict conformance with all applicable laws and with Vanderbilt policies governing confidential information. I understand and agree that measures must be taken so that all confidential information captured, maintained, or utilized by VUMC and any of its off-site clinics or affiliated entities is accessed only by authorized users. These obligations apply to confidential information that is collected or maintained verbally, in paper, or electronic format.

VUMC Confidential Information includes any and all of the following categories:

- Patient information including demographic, health, and financial information (in paper, verbal, or electronic form regardless of how it is obtained, stored, utilized, or disclosed);
- Information pertaining to members of the VUMC Workforce or Extended Community (such as social security numbers, banking information, salaries, employment records, student records, disciplinary actions, etc.);
- Vanderbilt University or VUMC information (such as financial and statistical records, academic or research funding, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary information including computer programs, source code, proprietary technology, etc.);
- Third-party information (such as insurance, business contracts, vendor proprietary information or source code, proprietary technology, etc.); and
- Patient, research, academic program, or other confidential or proprietary information heard or observed by being present on VUMC premises.

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

1. I will access, use, and disclose confidential information only as authorized and needed to perform my assigned job duties. This means, among other things, that I:
   a) will only access, use, and disclose patient or other Confidential Information that I have authorization to access, use, and disclose in order to perform my job duties;
   b) 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 duties and as in accordance with all applicable Vanderbilt policies and procedures and with all applicable laws;

c) will report to my supervisor and to the VUMC Help Desk any individual’s or entity’s activities that I suspect may compromise the privacy or security of VUMC Confidential Information.

2. If I am granted access to Vanderbilt electronic systems, including email, I am the only person authorized to use the individual user identification names and passwords or access codes assigned to me. I agree to the following:

a) To safeguard and not disclose my individual user identification passwords, access codes or any other authorizations that allows me to access VUMC Confidential Information to anyone including my manager, supervisor, or LAN manager.

b) To 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 any system to which I have 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 immediately change my password.

f) I understand that my user identification will be deactivated upon notification to Information Management that I am no longer a VUMC Extended Community Member; or when my job duties no longer require access to the computerized systems.

g) I understand that VUMC has the right to conduct and maintain an audit trail of all accesses to confidential 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 in order 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 Vanderbilt may at any time revoke my passwords or access codes.

i) I understand that individuals who access VUMC Confidential Information from home must follow Vanderbilt’s Security Guidelines for Remote Access.

j) I understand that in addition to protecting confidential information 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.

My signature below indicates that I have read, accept, and agree to abide by all of the requirements described above. I acknowledge that any violation of these requirements may result in suspension or termination of my rights to access VUMC systems and Confidential Information.

Signature: ____________________________ Date: ________________

Printed Name: ____________________________

Job Title: ____________________________ Company: ____________________________