myUNM Health

HIPAA Agreement Form

Provider Portal Request Guests (Non-HSC/UNM Health System workforce members) User Agreement/Authorization

By signing this document, I represent that:

1. I understand that Federal and state laws (i.e. HIPAA – See Appendix B) regulate the acquisition and access of protected health information and other personally identifiable information, and the use of computer facilities, electronically encoded data, and computer software.

2. I agree to limit my access and use of my UNM Health System (UNMHS) Guest Access Account to minimal necessary use to accomplish authorized work in support of the missions of the University of New Mexico Hospitals and the enhancement of information transfer to facilitate referred patient care.

3. I agree to complete a Privacy and Information Security Awareness and Education program annually, sponsored by my agency, corporation, university, and/or employer; or have completed the UNMHS Information Privacy and Information Security Awareness and Education Program.

4. Where I demonstrate a need to know and right to know, and I am granted access to the UNMHS's Protected Health Information (electronic medical records), I will take prudent and responsible measures to safeguard the information from unauthorized acquisition and access.

5. To comply with HIPAA, I agree to provide UNMHS written notice within five (5) calendar days of known or suspected unauthorized acquisition and access of individuals' protected information (i.e. a loss or breach of data entrusted to me, or my employer).

6. Where I am authorized to review UNMHS Protected Health Information, I will implement good information security controls to safeguard the confidentiality, integrity, and availability of the data as specified under the United States Health and Human Services HIPAA Privacy and Security rule.

7. I will report security incidents, issues, and any concerns in writing within five (5) calendar days to the IT Technical Support Center/ Helpdesk at 505-272-3282.

8. I understand that UNMHS maintains electronic access logs for company owned and managed electronic information systems and networks; and that representatives of UNMHS may routinely monitor and review these logs to safeguard the confidentiality, integrity, and availability of mission critical systems. I agree to provide information and documentation regarding any inquiries concerning my access to the UNM HSC Privacy Office.

9. I have access to, read, understand, and agree to abide by the UNMHS Guest Access System Users Responsibilities outlined in Appendix A (attached).

10. I understand that my USERID and password are to be used solely by me in connection with my authorized access. I agree to choose a difficult to guess password. I understand that I am required to sign off from the computer when I have completed authorized access, or when I physically leave the workstation, and that any access under my USERID and password by another person is my responsibility.

11. **NOTE: Your patients' data can be accessed by any myUNM Health Provider Portal user who has been granted a user account and has global search capability enabled. Users should only access data for patients for whom they are providing care.** Notification will be submitted to UNMHS immediately upon change in employment status to modify or terminate agreement, as deemed appropriate.

Applicant Printed Name _____

Applicant's Signature _____ **Date** _____

Applicant's Business Email Address _____

Practice Name _____

myUNM Health

HIPAA Agreement Form

Provider Portal Request Guests (Non-HSC/UNM Health System workforce members) User Agreement/Authorization

APPENDIX A

System Users Responsibilities: System users are responsible for:

a. Understanding, agreeing to and complying with all security policies governing University of New Mexico Health Systems (UNMHS) Computer and Network Resources and with all federal, state and local laws, including laws applicable to the use of computer facilities, electronically encoded data, and computer software.

b. Safeguarding passwords and/or other sensitive access control information related to their own accounts or network access. Such information must not be transmitted to, shared with, or divulged to others. Similarly, system users must recognize the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share, or divulge such information, nor convert the same from encrypted or enciphered form to unencrypted form or legible text. Any attempt to conduct such actions by a system user is a violation of this policy.

c. Taking reasonable precautions, including personal password maintenance and file protection measures, to prevent unauthorized use of their accounts, programs, or data by others.

d. Ensuring accounts or computer and network access privileges are restricted to their own use only. System users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorized computer and network access privileges to others. System users must not implant, execute, or use software that allows them unauthorized remote control of UNMHS Computer and Network Resources, or of accounts belonging to others.

e. Ensuring the secure configuration and operation of Internet services (e.g., WWW) they may establish on machines connected to UNMHS Computer and Network Resources. Also, system users are solely responsible for ensuring the content of files, programs, or services that they operate, maintain, store, or disseminate using University Computer and Network Resources (to include personally-owned computers connected to such resources) are compliant with both law and UNMHS Policy.

f. Using accounts or network access only for the purposes for which they were authorized. Use of accounts or network access to conduct a commercial enterprise, or to promote or advertise a commercial enterprise is prohibited. Transmitting or making accessible offensive, obscene or harassing materials, and transmitting or making accessible chain letters, etc., are prohibited. Unauthorized mass electronic mailings and newsposts are prohibited. Conducting or attempting to conduct security experiments or security scans involving or using UNMHS Computer and Network Resources is prohibited. The intentional or negligent deletion or alteration of information or data of others, intentional or negligent misuse of system resources, intentionally or negligently introducing or spreading computer viruses, and permitting misuse of system resources by others are prohibited.

g. Representing themselves truthfully in all forms of electronic communication. System users must not misrepresent themselves as others in electronic communications. Similarly, system users must not cause a system to assume the network identity or source address of another UNMHS Computer or Network Resource for purposes of masquerading as that resource.

h. Respecting the privacy of electronic communication. System users must not obtain nor attempt to obtain any electronic communication or information not intended for them. In particular, system users must not attempt to intercept or inspect information (e.g., packets) en route through UNMHS Computer and Network Resources, nor use UNMHS Computer and Network Resources to attempt to intercept or inspect information en route through networks elsewhere. Similarly, system users must not implant, execute, or use software that captures passwords or other information while the data are being entered at the keyboard or other data entry device.

i. Respecting the physical hardware and network configuration of UNMHS-owned or operated networks. System users must not extend the physical network on which their system resides (e.g., wiring, jacks, wireless connection).

j. Treating non-UNMHS Computer and Network Resources in accordance with this policy. UNMHS Computer and Network Resources must not be used to attempt to breach the security or security policy of other sites (either willfully or negligently).

myUNM Health

HIPAA Agreement Form

Provider Portal Request Guests (Non-HSC/UNM Health System workforce members) User Agreement/Authorization

APPENDIX B

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information ("PHI"), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Specific definitions include:

A. Disclosure. "Disclosure" shall mean the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

B. Electronic Protected Health Information. "Electronic Protected Health Information" means Protected Health Information that is created, received, maintained, or transmitted by Electronic Media as defined at 45 C.F.R. §160.103.

C. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160, 162, and 164, and as amended.

D. HITECH Standards. "HITECH Standards" shall mean the privacy, security, and Breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH") Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and any regulations promulgated.

E. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subpart A and Subpart E, as amended.

F. Protected Health Information or "PHI". "Protected Health Information or PHI" shall mean any information, transmitted or recorded in any form or medium; (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe that information can be used to identify the individual, and shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations and agency guidance. Protected health information excludes individually identifiable health information: (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.

G. Security Incident. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

H. Security Rule. "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Parts 160, 162, and 164, and as amended.

I. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

J. Any terms capitalized, but not otherwise defined, in this Agreement shall have the same meaning as those terms have under HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations, and the HITECH Standards.