This Agreement contains the terms and conditions that govern use of the Physicians Data Trust Web portal site applications by a provider (as defined below) for access to information on Physicians Data Trust member eligibility, claims payments and prior authorizations. This agreement is required for all providers and non-providers (provider representatives) who intend to use the Physicians Data Trust Web site applications at www.cerecons.com.

Definitions

In this Agreement, the words:

• "Authorized Representative" means a person that a Provider has authorized to use the web portal under this Agreement on the Provider's behalf.

• "Provider" means the person or entity registered with Physicians Data Trust to provide medical services or supplies to Physicians Data Trust enrollees.

•"Web portal" means, collectively, all services, functionality, content, and data made available by Physicians Data Trust through the Web site located at www.cerecons.com.

Terms of Site and Data Usage

Physicians Data Trust's web portal provides access to information on member eligibility, claims processing submission and status, referral submission and status and check status through the Internet. Use of the web portal is restricted to Providers and Authorized Representatives. Actual or attempted unauthorized use of the web portal will result in criminal or civil prosecution, in addition to any other available remedies.

Provider/Representative agrees to limit the usage of the web portal to the following eligibility, referral and claims-related transactions:

A. Verification of eligibility

B. Claims status information

C. Claims Submission

D. Referral status information

E. Referral Submission

F. Member profile information

Data provided through this website is protected health information

Data is made available only for patient treatment or payment purposes. Disclosure of this data other than for treatment and payment purposes is a violation of State and Federal law.

Access will be granted to individuals who have a need to gain access and will be terminated in line with staffing changes at the provider entity office.

Use of the Physicians Data Trust web portal will abide by Physicians Data Trust's compliance program

Security Requirements

The Provider/Representative agrees to the following security requirements. All computers that access Physicians Data Trust data must meet the following requirements, in addition to any State and Federal required administrative, technical, physical, and organizational safeguards:

1. Use of the Internet is solely at Provider's own risk and is subject to all applicable local, state, national, and international laws and regulations. While Physicians Data Trust has endeavored to create a secure and reliable site, Physicians Data Trust is not responsible for the security of information transmitted via the Internet, the accuracy of the information contained on the web portal, or for the consequences of any reliance on such information.

2. Physicians Data Trust will not be liable for any loss resulting from a cause over which Physicians Data Trust does not have direct control, including but not limited to failure of electronic or mechanical equipment or communication lines, telephone or other interconnect problems, interruption of communications or data processing services, unauthorized access, theft, operator errors, severe weather, earthquakes, or natural disasters, strikes or other labor problems, wars, or governmental restrictions.

3. System Timeout. The web portal will provide an automatic timeout, requiring re-authentication of the user session. The automatic timeout be after no more than 20 minutes of inactivity.

4. User Name and Password Controls. Systems that access the Physicians Data Trust web portal accessed using a unique user name. The user name must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be:

1. At least eight characters,

2. A non-dictionary word

(2) Not be stored in readable format on the computer or workstation,

(3) Be changed every 60 days,

(4) Be changed if revealed or compromised, and

(5) Be composed of characters from at least three of the following four groups from the standard keyboard:

• Upper case letters (A-Z)

• Lower case letters (a-z)

• Arabic numerals (0-9)

• Non-alphanumeric characters (punctuation symbols)

Release of Liability and Indemnification

In consideration for Physicians Data Trust's granting you permission to use the Physicians Data Trust Portal, you expressly release and hold harmless Physicians Data Trust, its trustees, officers, directors, employees, agents

and affiliates from any and all claims, liabilities, demands, causes of action, costs, expenses, and damages of every kind and nature, in law, equity, or otherwise, arising out of or in any way related to your use of the Physicians Data Trust Portal, or any of the data or other content obtained by using the Physicians Data Trust Portal, whether or not arising from any acts or omissions by Physicians Data Trust or its trustees, officers, directors, employees, agents or affiliates.

In addition, you shall indemnify and hold harmless Physicians Data Trust, its officers, directors, agents, affiliates, and employees, against all actual and direct losses, liabilities, damages, claims, costs or expenses (including reasonable attorney's fees) they may suffer as the result of third party claims, demands, actions, investigations, settlements or judgments against them arising from or in connection with any breach of this Agreement, or from any claim of any nature or any wrongful acts or omissions, by you or your Authorized Representatives or your other employees, officers or agents.

These provisions shall survive any termination of this Agreement.

Governing Law; Legal Jurisdiction; and Statute of Limitations

The laws of the State of California govern this Agreement, without regard to conflict of law principles, and your access to and use of the Physicians Data Trust Portal, and the data and other content obtained thereby, under this Agreement. You hereby submit to the exclusive jurisdiction of the courts in the State of California with venue in Orange County and waives any jurisdictional venue or inconvenient forum objections to such court.

STATEMENT OF CONFIDENTIALITY

I understand that it is the policy of Physicians Data Trust to respect and maintain the confidentiality of all Confidential Health Information with respect to all patients serviced by Physicians Data Trust. For purposes of this request, patient “Confidential Health Information” shall include without limitation, all Confidential Health Information regarding a patient's: (1) Medical treatment and condition; (2) Psychiatric and Mental Health; and (3) Substance abuse and Chemical dependency, and shall include without limitation, the following patient identifiable information: (1) Name; (2) Address, including street address, city, county, zip code and equivalent geocodes; (3) Names of relatives; (4) Names of employers; (5) Date of birth; (6) Telephone numbers: (7) Facsimile number; (8) Electronic mail address; (9) Social security number; (10) Medical record number; (11) Health plan beneficiary number; (12) Account number; (13) Certificate/license number; (14) Any vehicle or other device serial number; (15) Web Universal Resource Number (WURL); (16) Internet Protocol (IP) address number; (17) Finger or Voice prints; and (18) Photographic images; and (19) Any other unique identifying number, characteristic, or code which could be used, alone or in combination with other information, to identify an individual. I understand that in addition to patient Confidential Health Information, during the scope of my service relationship with Physicians Data Trust, it may be necessary for me to receive, review, and work with certain other confidential and proprietary information of Physicians Data Trust that may relate to Physicians Data Trust or its client's other business information and/or records regarding Physicians Data Trust's operations, business plans and employees. For purposes of this statement such information and patient Confidential Health Information defined above, are referred to herein collectively as “Confidential Information.”

ACCOUNT AGREEMENT

I understand that no Confidential Information may be accessed, discussed, or released without having the proper authorization to do so. Any access, discussions or release of Confidential Information shall only be for

purposes of patient care and/or client business and shall be on a “need to know” basis (i.e., in order to carry out the duties necessary for services provided to the patients and/or clients). Access shall also be limited to the "minimum necessary" information to achieve the purpose of the access. Access, disclosure or release includes, without limitation, the access of any electronic or paper-based Confidential Information. I further understand that I will be issued a unique Username and Password which I will keep confidential and will not reveal to anyone and that if I discover that the confidentiality of my Password has been compromised, I will change it immediately and promptly notify Physicians Data Trust. By indicating my signature below, I attest that I have reviewed and understand the foregoing statements and agree to be bound by the terms and conditions herein and the relevant Physicians Data Trust's policies and procedures regarding system access and confidentiality, and that any failure on my part to comply with the terms set forth herein and in such polices will be reported to my supervisor and may subject me to disciplinary action which may include immediate termination of my computer account(s).