



## IT SYSTEMS COMPUTER ACCESS AND CONFIDENTIALITY OF INFORMATION AGREEMENT

THIS IT SYSTEMS COMPUTER ACCESS AND CONFIDENTIALITY OF INFORMATION AGREEMENT (hereinafter "Agreement") is entered into with Floyd Healthcare Management Inc. (hereinafter "FHMI") by the undersigned physician or by the undersigned employee of a physician (such person who is executing this Agreement being hereinafter referred to as the "Undersigned"), effective as of the date set forth beside the Undersigned's signature.

**BACKGROUND:** FHMI has implemented various Information Technology systems which includes, without limitation, Cerner Millennium, Allscripts Touchworks, McKesson Physician Portal, McKesson STAR, McKesson HPF, GE GroupCast, and Fuji Synapse (hereinafter "IT Systems"). Physicians on the medical staff of FHMI and designated employees of such physicians can gain computer access to certain information either on site at an FHMI facility or from remote locations. The patient information accessible to physicians and their designated employees through the FHMI IT Systems consists of patient demographic information (including billing information) and patient clinical information (e.g., laboratory test results, x-ray/imaging interpretation reports, current diagnosis, etc.) (such information being hereinafter referred to as "Patient Information"). The Undersigned is either: (1) a physician on FHMI's medical staff who desires to utilize the FHMI IT Systems for purposes of having access to Patient Information respecting his/her patients, or (2) an employee of such a physician (or an employee of such physician's group practice) who has been specifically designated by his/her employer-physician as one who should have such access in order to facilitate the employer-physician's rendition of medical care of and treatment to patients.

**ACKNOWLEDGMENT AND AGREEMENT:** FHMI will assign to the Undersigned a unique user name and a unique password which will allow the Undersigned to access Patient Information through the FHMI IT Systems. In addition, some IT Systems may require a Personal Identification Number ("PIN") in order to access certain functions. In consideration for such access, the Undersigned acknowledges and agrees to the following:

1. As a physician with privileges at FHMI or any employee of such a physician, the Undersigned has a duty to protect the confidentiality of Patient Information. Therefore, any Patient Information to which the Undersigned is exposed within the course of his/her interactions with FHMI, including Patient Information accessed through the FHMI IT Systems, shall be treated by the Undersigned as highly confidential and shall not be disclosed to anyone other than the patient to whom such Patient Information pertains (or to such patient's authorized representative) or persons having need of the Patient Information in order to perform professional duties respecting the patient. Patient Information should not be accessed by anyone whose current professional duties do not require such access.

2. The Undersigned shall not access, use, or disclose Patient Information in a manner that would violate the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including, without limitation, the so-called Privacy Standards and Security Standards implemented pursuant to HIPAA and found in 45 CFR § 165.101, et seq. and 164.101, et seq.
3. The Undersigned will not disclose his/her unique user name, password, or PIN to anyone under any circumstances. The Undersigned will not write or otherwise document his/her user name, password, or PIN in any manner, which would allow them to be viewed by other persons.
4. When the Undersigned logs onto and gains access to Patient Information through the FHMI IT Systems, he/she will not allow any unauthorized person to view the Patient Information thereby accessed. When the Undersigned leaves the physical vicinity of a PC upon which he/she has logged onto the FHMI IT Systems, the Undersigned will ensure that he/she properly logs out of the FHMI IT Systems.
5. Use of the Undersigned's user name, password, or PIN by anyone other than the Undersigned is forbidden under any circumstances. A physician shall not allow his/her employees or any other person to access the FHMI IT Systems by using the physician's user name, password, or PIN; rather, any access by a physician's employee must be through such employee's own unique user name and unique password and unique PIN (if applicable). Only employees of a physician who are specifically designated by such physician shall be eligible to receive a user name and a password and a PIN (if applicable). If the Undersigned learns or has reason to believe that his/her user name, password, or PIN may be known by others, the Undersigned shall immediately notify FHMI's Medical Staff Office and its Information Technology Department. If the Undersigned learns or has reason to believe that any person has made any unauthorized access to the FHMI IT Systems, the Undersigned shall immediately notify FHMI's Medical Staff Office and its Information Technology Department.
6. The Undersigned is authorized to utilize the FHMI IT Systems only in connection with the Undersigned's own patients (or, in the case of an employee, in connection with the patients of his/her employer-physician). At no time shall the Undersigned utilize the FHMI IT Systems for any reason other than its intended use which is to perform professional duties respecting the Undersigned's patients. Any actual or attempted access by the Undersigned to Patient Information respecting patients other than his/her own patients (or, in the case of an employee, in connection with the patients of his/her employer-physician) shall constitute a breach of this paragraph 6 for which FHMI may seek such legal redress and damages as may be allowable under applicable law. Additionally, any such breach shall subject the Undersigned to disciplinary action by FHMI, including, but not limited to, revocation of the Undersigned's privilege to utilize the FHMI IT Systems and, in the case of physicians, corrective action under the FHMI Medical Staff bylaws.

7. The undersigned will ensure that appropriate security measures are implemented and maintained respecting any PC utilized by the Undersigned to access the FHMI IT Systems. Without limiting the generality of the preceding sentence, the Undersigned agrees that he/she will not cause or permit any Patient Information to be electronically downloaded, saved or otherwise stored on any such PC or any portable storage device connected to such PC, and the Undersigned will take all reasonable and practical measures to minimize the risk of unauthorized access to the FHMI IT Systems through such PC.
8. Any physician who designates an employee for purposes of having a user name, password, or PIN (if applicable) issued to such employee shall have the responsibility to immediately notify FHMI's Medical Staff Office and FHMI's Information Technology Department in the event the employment of such employee is terminated or in the event of any other change in circumstances which would make such employee's continued access to the FHMI IT Systems inappropriate.
9. The Undersigned will not attempt to learn another user's user name, password, or PIN; nor will the Undersigned use any user name, password, or PIN other than his/her own.



IT SYSTEMS COMPUTER ACCESS AND  
CONFIDENTIALITY OF INFORMATION  
AGREEMENT

Please check the appropriate box and complete all blanks in that section

I am a physician on the FHMI Medical Staff and I request access to the following FHMI IT Systems:

Printed Name

IT Systems Needed

Group Affiliation

Office Telephone Number

Physician Signature

Date

I am a person employed by the following physician and I request access to the following FHMI IT Systems:

NOTE: The supervising physician must also sign this agreement

Printed Name of Physician Employee

IT Systems Needed

Printed Name of Supervising Physician

Office Telephone Number

Employee Signature

Date

Physician Signature

Date

\*\*\*\*\* For use by Floyd Information Technology only \*\*\*\*\*

Application

User Name

Access Level

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_