CONFIDENTIALITY AGREEMENT REGARDING ACCESS TO ELECTRONIC MEDICAL RECORDS

THIS ELECTRONIC MEDICAL RECORDS ACCESS AND CONFIDENTIALITY AGREEMENT ("AGREEMENT") is made and entered into effective _____, between Advanced Inmate Medical Management, LLC ("AIMM") and _____ ("USER").

County and State: _____

RECITALS

A. AIMM creates and maintains demographic and health information relating to patients in correctional facilities (defined as "CONFIDENTIAL INFORMATION"). This CONFIDENTIAL INFORMATION is located in computer information systems as well as paper charts and files. The CONFIDENTIAL INFORMATION is protected from unauthorized or inappropriate access by AIMM policy, as well as state and federal law.

B. USER regularly provides healthcare services to patients in correctional facilities. These services can be provided more safely, effectively, and timely if USER has appropriate access to relevant CONFIDENTIAL INFORMATION maintained by AIMM.

C. In order to provide the best possible service to patients, AIMM wishes to grant USER appropriate access to CONFIDENTIAL INFORMATION contained in AIMM INFORMATION SYSTEMS as needed to provide healthcare for those patients. AIMM INFORMATION SYSTEMS is defined to include all AIMM computer hardware, software, data or voice communication facilities, excluding AIMM web pages devoted to employment job resources, and general public information.

The parties agree as follows:

AGREEMENT

1. **Access to CONFIDENTIAL INFORMATION through AIMM INFORMATION SYSTEMS.** AIMM agrees to provide USER with access to CONFIDENTIAL INFORMATION through the AIMM INFORMATION SYSTEMS, subject to the conditions outlined in this AGREEMENT. This access is provided to allow USER to obtain CONFIDENTIAL INFORMATION to the extent necessary to provide healthcare to patients under the care of USER and to permit effective and timely completion of medical records and orders.

2. **Scope of Use.** USER agrees not to gain access to, use, copy, makes notes of, remove, divulge or disclose CONFIDENTIAL INFORMATION, except as necessary to provide healthcare to patients under the care of USER and to permit effective and timely completion of medical records and orders. USER agrees to control the access and use of CONFIDENTIAL INFORMATION or AIMM INFORMATION SYSTEMS in a manner to comply with this AGREEMENT.

3. **Protection of Confidentiality and Security of CONFIDENTIAL INFORMATION.** USER agrees to protect the confidentiality and security of the CONFIDENTIAL INFORMATION obtained from AIMM. USER agrees to comply with applicable federal and state laws and with all existing and future AIMM policies and procedures concerning the confidentiality, privacy, security, use and disclosure of CONFIDENTIAL INFORMATION, which are available upon request.

4. **Codes and Passwords.** USER agrees not to release USER's authentication code or device or password to any other person or allow anyone else to access AIMM INFORMATION SYSTEMS under USER's authentication code or password. USER agrees to notify AIMM immediately if USER becomes aware or suspects that another person has access to USER's authentication code or device or password.

5. **Computer Security.** USER agrees to maintain adequate security procedures for the computers on which USER accesses the AIMM INFORMATION SYSTEMS. USER will abide by the minimum security and AIMM hardware and software desktop standards as set forth by AIMM. <u>USER understands that USER is prohibited from accessing and using AIMM INFORMATION SYSTEMS anywhere other than the correctional facility, unless specific permission is given to USER from AIMM for use at USER's home or other remote location.</u> USER will not use or attempt to access AIMM INFORMATION SYSTEMS by any means not specifically authorized by AIMM, including but not limited to the use of any Internet or non-secure means of connection. USER will take no action to avoid or disable any protection or security means implemented in

the AIMM INFORMATION SYSTEMS or otherwise use any means to access AIMM INFORMATION SYSTEMS without following log-in procedures specified by AIMM.

6. **Portable Media Devices.** USER agrees that if USER saves CONFIDENTIAL INFORMATION to portable media devices (Floppies, ZIP disks, CDs, PDAs, and other devices), USER will take reasonable safeguards to protect the devices and CONFIDENTIAL INFORMATION from any access or use not authorized by this AGREEMENT. If USER is uncertain on how best to protect CONFIDENTIAL INFORMATION, USER will contact AIMM on how to protect CONFIDENTIAL INFORMATION on the device while it is being serviced or repaired. USER agrees that if any portable media device needs to be reformatted or destroyed, USER will follow guidelines of AIMM for proper data cleansing or follow any policies or guidelines provided by AIMM for reformatting or destruction of electronic media.

7. **Printing CONFIDENTIAL INFORMATION.** If USER prints CONFIDENTIAL INFORMATION, USER will take reasonable safeguards to protect the printed CONFIDENTIAL INFORMATION from access or use not authorized by this AGREEMENT, and thereafter destroy such copies when they are no longer required for the purposes authorized herein.

8. **Return of Software or Equipment.** Upon request by AIMM, USER agrees immediately to return any software or equipment provided to USER by AIMM.

9. **Auditing Compliance.** USER agrees that USER's compliance with this AGREEMENT may be subject to review and/or audit by AIMM.

10. **Limitation of Liability of AIMM/Exclusions of Warranties.** The parties agree that USER is responsible for the ultimate decisions and medical judgment related to the diagnosis and treatment of his/her patients based on CONFIDENTIAL INFORMATION accessed on AIMM INFORMATION SYSTEMS. USER understands and agrees that remote access to electronic records involves technological risks, including possible introduction of errors, data corruption, and artifacts that may not be present on original versions of radiological results. USER understands that images accessed remotely may not have the same degree of clarity as images viewed on-site.

    USER agrees that AIMM will not be liable for any direct, indirect, incidental, special or other damages incurred by USER arising out of the remote use of or inability to use the AIMM INFORMATION SYSTEMS. AIMM does not guarantee or warrant the availability of remote access of AIMM INFORMATION SYSTEMS.

    The parties recognize that remote access introduces unique risks associated with unrelated software that may exist on the remote access device that compromises the integrity and security of data and remote access, including but not limited to spyware, hacker access, viruses, worms, and other harmful software (collectively referred to as "REMOTE ACCESS RISKS"). Accordingly, AIMM will not be responsible for any losses or damages related to REMOTE ACCESS RISKS.

11. **Response to Confidentiality Concerns.** Whenever AIMM in its sole judgment and discretion believes that USER has obtained unauthorized access to CONFIDENTIAL INFORMATION, has disclosed CONFIDENTIAL INFORMATION inappropriately or in violation of federal or state laws or regulations, has violated any AIMM policies or procedures regarding confidentiality or the use of CONFIDENTIAL INFORMATION, or has violated any provisions of this AGREEMENT, AIMM is also entitled to take any or all of the following actions immediately, as it determines to be appropriate:

    a. Suspend or terminate USER's remote access to AIMM INFORMATION SYSTEMS until AIMM concerns are addressed.

    b. Refer USER to AIMM per review process and report USER to a professional board, as appropriate.

    c. Terminate this AGREEMENT.

    d. Bring legal action to enforce this AGREEMENT.

12. **Continuing Obligations.** USER agrees that the obligations under this AGREEMENT continue in the event his or her medical staff privileges with the correctional facility are terminated or expire, or in the event AIMM terminates this AGREEMENT.

13. **Term and Termination.** This AGREEMENT shall be effective as of the date above, and shall continue in full force and effect until terminated under Section 11 of this AGREEMENT or with 30 days' written notice by either party. However, AIMM reserves the right to terminate USER's access to AIMM INFORMATION SYSTEMS at any time at their discretion

for reasons including, but not limited to, misuse of USER's access, failure to adhere to the conditions of this AGREEMENT or AIMM policies, or a breach of confidentiality. Furthermore, as an additional security measure, if USER has not logged in for a period of 60 days, USER's account will automatically be disabled.

a. If AIMM terminates this AGREEMENT, the USER's account will be disabled and no longer valid and USER will not have access to the electronic records. If USER terminates this AGREEMENT, USER's account will become inactive and he/she will no longer have access to the electronic records.

b. A USER who is no longer employed by the correctional facility is considered to have terminated this AGREEMENT.

14. Non-Assignment. Neither party may assign this AGREEMENT or their rights hereunder without the prior written permission of the other party.

15. Notice. All notices required by this AGREEMENT shall be in writing, and shall be deemed effective when personally delivered, five business days after being mailed by certified or registered mail, return receipt requested; or five business days after being deposited with a comparably reliable postage delivery service, such as Federal Express; addressed to the other party as follows:

If to AIMM: Legal Dept.
c/o AIMM
3922 W Baring Trace
Peoria, IL 61615

If to USER: _____
_____
_____

16. Waiver. Any waiver of any of the terms or conditions of this AGREEMENT by any party shall not be construed as a general waiver of the same condition for any subsequent breach.

17. Additional Safeguards. USER understands and agrees that the HIPAA Security Regulations require AIMM and USER to implement security and privacy processes, practices and technical requirements in connection with the access and use of electronic CONFIDENTIAL INFORMATION. AIMM reserves the right to impose additional security safeguards, including without limitation software and hardware requirements, to comply with the Security Standards. If USER elects not to adhere to these new requirements, USER and/or AIMM may terminate this AGREEMENT pursuant to Section 11 above.

18. Governing Law. This AGREEMENT shall be governed by and construed in accordance with the laws of the State of Illinois. Jurisdiction and venue shall be Peoria County, Illinois.

IN WITNESS WHEREOF, this AGREEMENT has been executed on the day and year first above written.

ADVANCED INMATE MEDICAL MANAGEMENT, LLC

_____ _____
Norman Johnson Date
Member

USER:

_____ _____
Signature Date

_____ _____
Printed Name County and State