Decatur Morgan Hospital

CLINICAL INSTRUCTOR INFORMATION FORM

Name: _____

Address: _____

_____

Date of Birth: _____ Gender: _____

Contact Phone Number: _____

Emergency Contact: _____

Emergency Contact Phone Number: _____

Email: _____

School: _____

❑ I am currently employed by Decatur Morgan Hospital

Department/Area _____

Start Date: _____ End Date: _____

*** ALL FORMS NEED TO BE UPDATED ANNUALLY FOR CONTINUED ACCESS ***

For Staff Only:

❑ Copy of Driver's License

Decatur Morgan Hospital

Access Request Form
Print Legibly

___Provider ___MD Office Staff ___Employee ___Vendor ___Student

***Name – Last, First, Middle Initial (as filed in Human Resources)** _____ **Credentials MD, RN, PA, Etc…** _____

***Employee ID** _____ **OR** ***Last 4 Digits of SS#** _____ ***Personal Contact Phone** _____

***Department** _____ **OR** ***Company Name/Office/Practice Name** _____ ***Work/Office Phone** _____

***Email Address USE YOUR HOSPITAL EMAIL ADDRESS IF YOU WERE ISSUED ONE**
***required**

Select desired Meditech system access level below (Patient Medical Record)	**Other System Access**
___ Physician	**___ Internet Access**
___ ALP CRNP/PA (Advanced Practitioner)	**___ Email Account**
___ LC (Licensed Clinician)	**___ Pyxix ES AD**
___ CL (Clerical/Office Support)	**___Other _____**
___ MGR/MR (Manager, Med Rec)	**If replacing someone who:_____**
___ Student	**_____**
___ Other (Provide job Title)	**_ If temporary access request, expected date of termination:_____**
_____	**Remote Access Needed: Y N**

Comments: _____

Setup Requestor like the following employee: _____

Approval	**For Information Systems use only**
_____	**___ Add to a VM**
Signature of Director, VP, or Staff Physician	**___ Create an Active Directory Account**
Print Name:_____	**New Active Directory Account_____**
Date:_____	**___ BAA on file**

Fax completed Forms to: 256-973-3457

Call The IS HelpDesk for Assistance at 256-973-2115

Do not write below for Decatur Morgan Hospital Information Systems use only

Date Received at HelpDesk:_____ Approved:_____ Added:_____

Decatur Morgan Hospital

Access Agreement
Information Systems Department

In accessing, I agree to adhere to the DMH privacy and security policies and to the following conditions:
INITIAL EACH STATEMENT

A. ___ Passwords. Users are responsible for keeping all login user IDs and passwords secure. Logins are not to be shared under any circumstances. The user is responsible for information obtained using their login.

i. The user should choose a password that is not easily associated with the user.

ii. Human Resources will notify IS of all DMH employee terminations. This will allow IS to remove access privileges. Likewise, physicians and third parties are responsible for notifying the IS Help Desk when employees with access are terminated.

iii. The user is responsible for notifying Director of IS promptly when login information has been compromised.

iv. Minimum password length is 8 characters with a mix of alphabetic characters and at least one numeric digit and/or special character.

v. Passwords are required to be changed on a rotating basis.

vi. Failure to maintain confidentiality of individual passwords, in accordance with this policy, will result in the forfeiture of access to DMH information systems.

B. ___ Failed Attempts. A connection shall be terminated after exceeding the failed login attempts limit.

C. ___ Replication of Data. Any information viewed through the system is strictly confidential and may not be copied, saved to any remote or portable device, disclosed to or shared with any other person for any purpose, except as specifically permitted by law.

D. ___ Audits. Access use will be audited on a routine basis**.**

E. ___ Logging Off. The user is responsible for logging off of the session when the workstation is unattended. Workstations/devices are programmed to automatically log off if they are inactive for 10 minutes.

F. ___ Dormant Accounts. The account may be closed after 90 days of non-use.

G. ___ Posting of Access Numbers. Information regarding access to computer and communications systems, such as dial-up modem phone numbers and Internet URLs shall not be posed on the Internet, listed in telephone directories, placed on business cards, or otherwise made available to third parties without IS proper approvals.

H. ___ Modems. Connection of a modem to a PC on the DMH network by anyone other than a member of the IS Network Team is prohibited. All dial-up connections with systems and networks shall be routed through a modem pool or RAS. Under no circumstances shall dial-up modems be connected to workstations that are simultaneously connected to a local area network (LAN) or another internal communication network. Exceptions may be authorized with the approval of the IS Director and appropriate department management. In the event that a dial-up connection for a workstation is approved, users shall not leave modems connected to personal computers in "auto-answer" mode.

I. ___ Workstation Use. Users shall adhere to software license agreements and DMH policies. Preparations shall be made to ensure that all work sites, including a home office, is appropriate for the work to be performed. Reasonable precautions shall be taken at alternative work sites to protect DMH owned hardware, software, and information from theft, damage, and misuse.

J. ___ Organizational Equipment. Equipment provided by DMH shall not be altered or added to in any way (e.g. upgraded processor, expanded memory, software or peripheral devices) without approval from the IS Director.

K. ___ Inspections. Devices that access the DMH network may be inspected at any time—given one-day advance notice—by the organization to insure data integrity. DMH information and/or data stored on remote devices are the property of DMH.

L. ___ Device Approval. In order to mitigate the propagation of viruses, prevent disputes about ownership, and reduce improper removal/theft; equipment or software not owned by the organization is prohibited from being used within the organization's facilities without prior IS management approval.

M. ___ Anti-Virus Software. Users are responsible for maintaining updates to commercially reasonable anti-virus and anti-spyware software.

N. ___ Reporting Incidents. In the event that any confidential information, including PHI, is intentionally or unintentionally disclosed or if equipment is lost or stolen, notify I.S., the Privacy Officer, or the Security Officer promptly.

O. ___ Printing. Remote printing is discouraged, except when expressly needed to perform HIPAA permitted functions of treatment, payment and operations. Any extraneous hard copy of confidential information, including PHI, should be shredded or otherwise destroyed after usage. Devices or documents containing confidential information should not be disposed of in household, physician office or third party trash. If proper means of destruction are not available, deliver device or documents to the DMH data center.

P. ___ Print Destination. Printing from or to a remote device creates uncertainty as to the destination printer; please verify where remote printing will take place before attempting to print confidential information, including PHI. In the event that you print to an unintended destination, notify the unit/office personnel and ask that the pages be destroyed. If the information is printed to an unknown destination, notify the privacy officer promptly.

Q. ___ Billing Information. Information needed for billing purposes may be used solely for the purpose of preparing an officially recognized claim form for reimbursement from any payer.

R. ___ Clinical Information. Clinical information may be used only for the approved purpose of continuity of care as permitted by federal HIPAA regulations.

S. ___ HIPAA Violations. Anyone violating patient privacy and patient confidentiality may be punished by civil or criminal penalty (including fines up to $250,000 and imprisonment) under federal law. Inappropriate access may be reported to the Office of Civil Rights for action.

T. ___ Compliance. Failure by any party (including employee, physician or physician office staff or authorized third party) to maintain patient, business or employee confidentiality as defined in Decatur Morgan Hospital HIPAA, security, and confidentiality related policies; and in accordance with state and federal laws will result in the forfeiture of access to DMH Information Systems. Reinstatement is at the discretion of the DMH IS Director and Sr Leadership Team**.**

U. ___ Disciplinary Action. Decatur Morgan Hospital employees violating privacy or confidentiality terms outlined in this policy will be subject to disciplinary action, up to and including dismissal.

V. ___ Physician Office Personnel. Physicians are responsible for the actions of their office staff as relates to hospital confidential information, including PHI. Should a violation of hospital privacy, confidentially or security policy occur: access will be terminated, the physician will be contacted, and the physician will be responsible for taking appropriate action.

W. ___ Support. For Remote Access support, call the IS Help Desk 256-973-2115

X. ___ Signed Affirmation Statement. Attached for Vendors and Physician Offices**.**

Failure to adhere to the above mentioned criteria will cause termination of access rights, and for employees, disciplinary action up to and including termination. HIPAA violations may be punished by civil or criminal penalty under federal law.

I have reviewed/initialed the conditions for access to Decatur Morgan Hospital Information Systems and agree to all the terms listed above.

User Signature_____ **Date**_____

Printed Name_____

Affiliation _____

Witness Signature _____ **Date**_____

Fax or scan completed forms to Decatur Morgan Hospital 256-973-3457
Call the Decatur Morgan Hospital IS Help Desk for assistance at 256-973-2115

Effective March 1, 2014
Last Revision date: October 1, 2015

Decatur Morgan Hospital

Non Employee Confidentiality Agreement

I agree that any disclosures of, unauthorized use of and/or unauthorized access to Confidentiality Information which could cause harm to the Hospital, including harm to it's reputation, is a violation of hospital policy and may result in disciplinary action, including termination of agreement/contract, depending on the circumstances.

1. To use Confidential Information for the sole purpose of performing the duties for which my agreement/contract designates.

2. Not to disclose any Confidential Information to any person whatsoever, except in direct connection with the performance of the designated terms of the agreement/contract.

3. Not to copy or reproduce, or permit any other person to copy or reproduce, in whole or in part, any Confidential Information other that in the regular course of the services I am authorized and requested to perform for the hospital.

4. To comply strictly with all hospital policies regarding security of the Confidential Information.

5. To report immediately to the Hospital any unauthorized use, duplication, disclosure, and/or dissemination of confidential Information by any person including myself.

I agree upon termination of my agreement/contract with the Hospital for any reason, I will immediately return any documents of other media containing any Confidential Information to the Hospital, and I will certify in writhing that all such documents and other media have been returned to the Hospital.

I understand that disclosure of any Confidential Information may cause the Hospital irreparable harm, for which monetary compensation may not be an adequate remedy, and that the Hospital may seek injunctive relief if I breach or attempt to breach the Agreement.

Further, I agree to indemnify the Hospital fully for any and all damages, including legal fees, the Hospital may incur as a result of my breach of this Agreement.

I agree that all my obligations under this Confidentiality Agreement shall survive termination of my agreement/contract with the Hospital, regardless of the reason for such termination.

Signature Date Print Name

Date: _____

Decatur Morgan Hospital

PYXIS ES USER FORM

Name: _____ _____ _____
First Middle Last

Decatur Campus	Parkway Campus
❑ CIC/ Vein Center	❑ PW – ED
❑ 4N & 4N2	❑ PW – LD
❑ 3N 3N2	❑ PW – Nursery
❑ ICU/CCU	❑ PW – WC
❑ Dialysis	❑ PW Med Surg (2N)
❑ OPS	❑ PW – ICU
❑ OR	❑ PW – OR
❑ PACU	❑ PW – PACU
❑ A-Systems	❑ PW – A Systems
❑ Cath Lab	
❑ ED	**West Campus**
❑ Infusion	❑ West
❑ Nuclear Medicine	
❑ Radiology	
❑ Respiratory	

❑ **Pharmacy access to all machines**

User Role:		
❑ Anesthesia	❑ DMH OB RN	❑ Pharmacy Floor Tech
❑ Anesthesia Tech	❑ DMH OR RN	❑ Pharmacy Tech
❑ Cath RN	❑ DMH RN	❑ Pharmacy Tech LEAD
❑ Cath Tech	❑ Echo	❑ Radiology / Imaging
❑ Charge Nurse / Manager	❑ Nurse Instructor	❑ Respiratory
❑ DMH ED RN	❑ Pharmacist	❑ West Nurse

PYXIS Training Date: _____ **Signature of Trainer:** _____

Access should match (other employee with same): _____

Signature of user: _____

Pyxis BIO-ID and Password are considered user signature.

Signature: _____ **ext:** _____
(Nurse Director/Nurse Educator)