St. Dominic's

APPLICATION for RESIDENTS and ROTATING STUDENTS

Anticipated Start Date: _____

Phone: (601) 200-6846 • Fax: (601) 200-0773

Returning? No

1. Identifying Information

Legal Last Name:	Legal First:	Legal Middle:	Degree:
Is there any other names under which you have been known (AKA/Maiden Name)? Name(s):			
NPI Number (if applicable):		Taxonomy Code: 390200000X	
Email Address:		Cell Phone Number:	
Date of Birth:	Sex:	Social Security #:	

2. Clinical Rotation Information

Supervising Physician Name:	Specialty:
Dates of Rotation:	

Classification:

Student:
- ☐ MD/DO Student
- ☐ NP Student
- ☐ PA Student
- ☐ Nurse Anesthetist Student
- ☐ First Assist Student

Resident:
- ☐ PGY1
- ☐ PGY2
- ☐ PGY3
- ☐ PGY4
- ☐ PGY5 and above

Name of Program Coordinator:
_____

Institution Name:
_____

Phone:_____ Fax:_____ Email:_____

Please include the following additional information when submitting the application:

- Current CV
- Current Professional Malpractice Certificate of Insurance

FMOLHS
INFORMATION SECURITY AND CONFIDENTIALITY AGREEMENT

Patient, financial, and other business-related information in any form, verbal, electronic or printed, is a valuable asset, and is considered private and sensitive. Employees, physicians, physician office staff, consultants, vendors, contracted agency staff, and students may have access to confidential information in the performance of their duties. Those charged with this responsibility must comply with information confidentiality/security policies in effect at FMOLHS and its affiliates (collectively referred to as "FMOLHS" in this Agreement). This agreement applies regardless of the method of access used.

As a condition to my association with FMOLHS, I agree to maintain the confidentiality of FMOLHS's confidential and proprietary information, including but not limited to:

1. Patient Information, including demographic, health and financial information.
2. Private information about members of FMOLHS's workforce (e.g. social security numbers, dates of birth, banking information, employment records, home addresses, and telephone numbers).
3. FMOLHS's proprietary and confidential information (e.g., trade secrets, patient lists, prices, professional fees, reimbursements, computer systems technology, profit and loss data, investments, sources of academic or research funding, proprietary research information, strategic and business plans, vendor/third party payor contracts, vendor lists, and peer review information).

As a condition to my access to FMOLHS information systems and my association with FMOLHS, I agree to the following conditions:

1. I understand that FMOLHS has the right to monitor data and information that are stored or communicated via the FMOLHS network and systems to ensure that all applicable laws and FMOLHS policies are followed. As such, I understand that, except as otherwise stated herein, there is no expectation of privacy on my part for any device that is connected to the FMOLHS network or systems or for any access to/from such systems. I also understand that all access may be monitored on the FMOLHS network.
2. I agree to abide by all present and future confidentiality/security policies and procedures including but not limited to the Mobile Device Policy; The Security Policies for the FMOLHS Information Network, The FMOLHS Internet/Email Access and Email Usage Policy, and the Physician Practice IS Services Policy (as relevant).I understand that such policies and procedures are available on the Intranet or have been provided directly to me.
3. I agree to comply with all applicable state and federal laws.
4. I will not operate or attempt to operate computer equipment without specific authorization.
5. I will not demonstrate the operation of computer equipment or applications to anyone without specific authorization.
6. I will not deliberately sabotage computer equipment or software, make or distribute unauthorized copies of software, or load unlicensed software or software unauthorized by FMOLHS on any computer belonging to FMOLHS.
7. I agree to maintain a unique password, known only to myself to access the system to read, edit and authenticate data. I understand that my unique password constitutes my electronic signature and that it should be treated as confidential information. I agree not to share my password with any other individual or allow any other individual to use the system once I have accessed it. I understand that I may change my password at any time.
8. I agree only to access the patient, financial, and/or other FMOLHS business-related information needed for the performance of my duties and responsibilities. Note: Internet access and appropriate usage is governed by a separate policy.
9. I will contact my FMOLHS representative, my supervisor, Chief Information Security Officer (CISO), or the FMOLHS IS department if I have reason to believe the confidentiality and security of my password has been compromised.
10. I will not disclose any portion of the computerized systems to any unauthorized individuals. This includes, but is not limited to, the design, programming techniques, flow charts, source code, screens, and documentation created by employees, outside resources, or third parties.
11. I will not disclose any portion of the patient's record except in accordance with FMOLHS's policies related to the release of patient records.
12. I understand that applications are available outside of the FMOLHS network via various remote access methods (i.e. VPN, Citrix, and/or Web), and I agree to abide by the following when accessing FMOLHS computer systems from remote locations: a. I will only access FMOLHS computer systems from remote locations if I am authorized to do so.
    b. I will use discretion in choosing when and where to access FMOLHS computer systems remotely in order to prevent inadvertent or intentional viewing of displayed or printed information by unauthorized individuals.
    c. I will use proper disposal procedures for all printed materials containing confidential or sensitive information.
    d. I understand that if I choose to use my personal equipment to access FMOLHS computer systems remotely, it is my responsibility to provide internet connectivity, configure firewall and virus protection appropriately, and to install any

necessary software/hardware. FMOLHS is not responsible if the installation of software necessary for accessing FMOLHS computer systems remotely interferes or disrupts the performance of other software/hardware on my personal equipment.

e. I understand that by using my personal equipment to access FMOLHS computer systems that my computer is a de facto extension of the FMOLHS network while connected, and as such is subject to the same rules and regulations that apply to FMOLHS owned equipment.

13. I agree to report any activity which is contrary to FMOLHS policies or the terms of this agreement to my supervisor, the CISO, or a security administrator.
14. If I will be using a mobile device to access the FMOLHS network or network services (through a personally-owned or FMOLHS owned device) that include, but is not limited to, email, VPN, or other remote access capabilities, I will allow FMOLHS limited control of my mobile device for the protection of FMOLHS data and its assets. For this context a mobile device is currently identified as a mobile phone, tablet, or other miniaturized computing system. This limited control can include the enforcement of a password/pin and/or remote wiping of the mobile device in the event of loss or theft or other factors that may present a risk of harm to the FMOLHS network, its data, or applications.
15. I agree to comply with all relevant FMOLHS Compliance and IS Policies, including but not limited to the Mobile Device Policy.
    a. In the event of loss or theft of my device, I agree to the remote wiping of all content on my mobile device, including any personal information I may have stored on the device, such as (but not limited to) photos, videos, and other content stored on the hard drive of the device.
    b. In the event of an investigation or inquiry by the internal compliance department or the government, or in the event of litigation, I agree to provide FMOLHS and/or its affiliate(s) with access to my device to copy and retain information related to the investigation, inquiry or litigation. I understand that FMOLHS will take reasonable steps to limit access to personal information, such as using key word searches to identify relevant material.

I understand that I must sign this Agreement as a precondition to issuance of a computer password for access to the FMOLHS network and/or patient information and that failure to comply with the preceding provisions will result in formal disciplinary action, which may include, but will not be limited to, termination of access, termination of employment in the case of employees, termination of agreements in the case of contractors, or revocation of clinical privileges in the case of medical staff members, taken in accordance with applicable medical staff by-laws, rules and regulations.

USER GETTING THE ACCESS – PLEASE PRINT & COMPLETE THIS SECTION:

Name of User:_____
(Please print the First name, Middle Initial, and Last name)

User Signature: _____ Date: _____ Email Address: _____

Last 4 digits of SSN: _____ Date of Birth: _____
*** This SSN and date of birth information requested above is to be used only for identification and auditing purposes. Only FMOLHS personnel who have a legitimate business reason will have access to this information. The Personal Information will be securely guarded and will not be disclosed to any third party.*

Job Title: Resident (Rotating Student)

Company Name: Medical Staff Services Contract Company Phone: (601) - 200 - 6846

OFFICE CLINIC MANAGER (Management Employee) – PLEASE COMPLETE THIS SECTION:

FMOLHS Requestor Name (Printed): Paula McCrory, Director Medical Staff Services Date: _____

FMOLHS Requestor Signature: Paula McCrory
As clinic manager, by signing above you acknowledge that all appropriate paperwork has been signed.

End Date: All End Dates are scheduled for June 12th and will extend when approved during the annual audit. If this person is no longer part of St. Dominic's/FMOLHS, please open a ticket for IT Provisioning Team to disable their access.

Remote Access/ VPN Request Form

St. Dominic-Jackson Memorial Hospital Information Technology, Security Group

Prerequisites

The Requestor, whether an internal workforce member or external vendor, must have an authorizing sponsor and a valid need for secure, remote access to the St. Dominic network.

For internal users (workforce member), submission by the workforce member's supervisor of an online security request form must accompany this request. This online form is located on the internal intranet. Contact the Helpdesk at 601-200-4000 for assistance.

Instructions

1. **Requestor (Remote User)** - Please fill out this form completely. Incomplete forms will be returned and fulfillment of your request will be delayed. Please forward the completed form as an email attachment to your Authorizing Supervisor or for external requestors, your St. Dominic Sponsor, for their approval.
2. **Two (2) Factor Authentication Required** – For security reasons St. Dominic's Hospital requires all remote connections to be authenticated using two (2) factor authentication. You must not only know your username & password to access St. Dominic's network but you must also have your cell phone or access to your work phone to authenticate each remote access session. Provide a cell or direct work phone as your PhoneFactor contact #.
3. **Authorizing Supervisor (Sponsor)** – If you approve this remote access request, forward this completed form as an attachment to itsecurity@stdom.com. All approvers/sponsors must be hospital employees and authenticated security requestors.
   NOTE: Access approved for a vendor or any other outside party will require an expiration date. Renewal of the requested access will be required on expiration.
4. **IT Support/Helpdesk –** Create ticket for the Security Group, priority: 3, category: Security; Remote Access, unassigned. Attach this form and other related forms to the ticket for their review.
5. **Security Group –** Verify the form is complete.. Retain all forms in the security file. For external vendors, create a remote user AD account. Add the user to the remote access group. Remember to include the expiration date for external users. Close the ticket. Contact the remote user with instructions. Notify the Vendor and/or sponsor the work is completed.

1. Contact Information

Account Sponsors and external vendors are to complete the "External Vendor" section. The Account Sponsor must be a member of the hospital or St. Dominic Health Services workforce and should be at the manager, director, or department head level.

External Vendor	Requestor (Remote User)	Account Sponsor and Department (only list once)
Name:		Paula McCrory
Title:		Director, Medical Staff Services
Phone Number:		601-200-6882
Cell Number:		662-315-1167
Email:		pmccrory@stdom.com
Two digit state identifier and last 4 digits of EIN		
Company:	St. Dominic Hospital | Medical Staff Services	St. Dominic Hospital | Medical Staff Services
Affiliation:	Resident/Rotating Student	
Expiration Date:		

2. Purpose of the Remote Access

Please answer the following questions about the purpose and criticality of the remote access you have requested.

Question	Answer
Please describe in general terms the purpose of this remote access, or the activities to be performed.	Cerner Access
Does this activity support official business functions of a department?	Yes
Is this activity critical to a department?	Yes
Are there feasible alternatives to remote access to achieve the same goals?	No
Are the functions to be performed part of the remote user's official job role?	Yes

3. Systems/Applications to be Accessed

Please fill in a row for each system that will be directly accessed by the remote user. Add additional rows if you need them.

IP Address	Hostname	Function	System Owner Approval Granted?

4. Remote Device Security Requirements - Disclosure

St. Dominic security policy sets minimum security criteria for all PCs that attach to St. Dominic networks. Remote clients attach to St. Dominic networks so they must also meet the relevant security criteria.

The Remote Access device may run "hostchecker software" to check for the presence of operating system patches, firewall, and anti-virus programs. As a user you are still obligated to follow and confirm that you will follow St Dominic security policies and procedures:

Question	Answer
Are strong passwords enforced for all accounts capable of logging into the remote device that will be used to access our network?	Yes
Is the sharing of passwords strictly prohibited?	Yes
Can the operating system distinguish between privileged administrative accounts and normal user accounts?	Yes
Is administrative access granted only to individuals who need it to perform official job functions?	Yes
Do users with administrative accounts also have normal user accounts which they use for all non-administrative functions?	Yes
Are the operating system and applications kept up to date with service packs and security patches?	Yes
What operating system and service pack are installed on the remote computer?	Unknown
Have unnecessary network services been disabled or uninstalled?	Yes
Has the system logging been configured to record security events such as logon/logoff, failed access attempts, shutdown/startup, and changes to logging	Yes

parameters?	
Is the device protected by active filters or firewalls?	Yes
Is the device protected by active anti-virus software that updates its virus definition files at least daily?	Yes

5. Requestor Statement of Acceptance

The information provided in this request form is accurate to the best of my knowledge. I understand that providing access to remote users and devices exposes St. Dominic to certain security risks. I will not conduct any activity that is considered in violation of the provisions set forth in HIPAA, HITECH or the Omnibus Rule. I agree to notify the St. Dominic Security Group when this account is no longer needed so the access can be disabled. I will also notify the St. Dominic Security Group if I become aware of any security problems or threats related to this remote access.

Signature _____ Date _____

6. Account Sponsor Statement of Acceptance

The information provided in this request form is accurate to the best of my knowledge. I understand that providing access to remote users and devices exposes St. Dominic to certain security risks. I accept responsibility for the risks imposed by the remote users I sponsor. I agree to notify the St. Dominic Security Group when this account is no longer needed so that the remote access can be disabled. I will also notify if I become aware of any security problems or threats related to this remote user.

Signature  Date _____

7. Security Group Use Only

Security Group: please fill out this section of the form for tracking purposes.

Ticket Number:	
Security Analyst:	
Type of remote access granted: ie. VPN, Citrix Gateway, Portal	
Request Form Received Date:	
Approval Status:	
Approval Date/Access Granted:	
Business Associate Agreement on file for external vendor, as required:	
Vendor credentialing for external vendor, as required:	

St. Dominic Information Technology
Support/Helpdesk Line 601-200-4000

Submit Form