

**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 Firstname, Middle Initial, and Lastname)*

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.\*\**

Company Name: \_\_\_\_\_ Contract Company Phone: (\_\_\_\_) - \_\_\_\_ - \_\_\_\_\_

**FMOL HEALTH SYSTEM SPONSOR (Management Employee) – PLEASE COMPLETE THIS SECTION:**

FMOLHS Requestor Name (Printed): \_\_\_\_\_ Date: \_\_\_\_\_

FMOLHS Requestor Signature: \_\_\_\_\_

*As FMOLHS Sponsor 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 Access Audit Portal (AAP). If this person is no longer part of FMOLHS, please open a footprints ticket for FMOLHS IS Provisioning Team to disable their access.

**CONTRACT PERSONNEL: Signed forms for contract Personnel should be**

1. **Submitted by the FMOL Health System Sponsor (Management Employee).** (A management employee should submit the request for access. Contract employees or non-management personnel cannot submit requests for access.)
2. **Attached to an IS Ticket** (Fax can be used: 225-765-9904)