

John Muir Health Link

John Muir Health Link Confidentiality Agreement Each user must sign and return a copy of this agreement.

This agreement applies to all JMH Systems. These systems contain medical records, diagnosis, test results, financials and other sensitive data of JMH patients and/or family members. This is data must be protected to comply with globally recognized standards, regulations, and business requirements, including HIPAA, HITECH, HiTrust, NIST, ISO, PCI, FTC, COBIT, and State laws. Please sign at the bottom to acknowledge that you have read and understood each of the following provisions.

1. I shall protect the confidentiality of the information contained in the JMH Systems as required by this Agreement and by applicable laws governing privacy and security of patient information, including but not limited to HIPAA and similar regulations.
2. I shall safeguard my JMH Systems user IDs and passwords (Credentials). I will not share my Credentials with any individuals (e.g., Supervisors, Contractors, etc.) or use another individual's Credentials to access JMH Systems.
3. I am being granted access to JMH Systems solely for the purpose of performing work-related duties. I will access the minimum amount of information authorized and necessary to perform such my work duties. I shall not use my JMH Systems account access for any personal or other purpose.
4. If I discover or suspect my JMH System Credentials have been compromised, I will immediately notify the JMH ITS Service Desk by calling (925) 941-2222 or emailing Support.Center@johnmuirhealth.com.
5. JMH conducts routine access audits to ensure information accessed through JMH Systems is appropriate. I understand that I am personally accountable for any actions taken using my Credentials.
6. JMH Systems contain confidential information and proprietary materials owned by JMH and/or JMPN and/or their respective licensors, such as Epic Systems Corp (collectively, JMH Confidential Information). I understand that JMH Confidential Information does not belong to me.
7. I shall not use or disclose any JMH Confidential Information with other individuals unless required to perform my work. If any such use or disclosure is required, I will follow the applicable procedures and instructions of my Supervisor or Director.
8. If I receive a request or demand from any person or organization other than JMH, or JMPN for JMH Confidential Information or access to the JMH Systems, I shall immediately notify the JMH Privacy Officer at (925) 941-2688 and my Supervisor.
9. I will not print, store, process, transmit, download or make copies of any information, software or screen shots accessed in the JMH Systems, except for copies required to document the treatment in the medical record maintained by a practice office or in the financial records maintained by a practice office to obtain payment for such treatment.
10. I understand that failure to comply with these requirements may result in revocation of my JMH Systems user account and other actions by JMH, and/or JMPN, including referral to appropriate law enforcement agencies.
11. Upon termination of my employment, service or engagement with the affiliated practice or organization or entity, I will return my Credentials to the JMH Systems (e.g., tokens) and all copies of documents containing JMH Confidential Information in my possession or under my control.
12. I have completed my organization's HIPAA Privacy & Security compliance training, and I will abide by to the applicable policies and procedures as they apply to accessing confidential information.

By signing below, I agree to comply with the requirements set forth above

Users Signature:	Title:
Users Printed Name:	Date: