Frequently Asked Questions about PATHWAYS Clinical Data Performance Platform

Basic Information	
Vendor	M2S
Application name	PATHWAYS Clinical Data Performance Platform
Application supports the following business functions	The Vascular Quality Initiative® (VQI®) utilizes M2S's PATHWAYS secure, cloud-based clinical data performance platform and is governed by the SVS Patient Safety Organization (SVS PSO). Collecting data on major vascular procedures, the Initiative offers an opportunity for data collection critical to meaningful long-term outcomes assessment.
Vendor address	12 Commerce Ave. West Lebanon NH 03784
Contacts	• Security Officer: Erik Linstad, ELinstad@m2s.com, 603-298-5509 x401 • Privacy Officer: Kathy Coughlin, coughlin@m2s.com, 603-298-5509 x342 • hipaa@m2s.com

Set-Up	
What are the OS requirements?	N/A, no client needs to be installed at the desktop level
What are the options for hosting this application?	PATHWAYS is a web-based system hosted at M2S which is securely accessed over the internet by hospital staff. The application has a web-tier and database backend.
What is the preferred configuration?	The application is a browser-based application hosted at M2S.
What are the browser requirements?	Most current versions of Internet Explorer, Firefox, Chrome, etc. are recommended.
What are the plug in requirements?	Flash Version 9 or higher.
Are there known compatibility issues with browser plugins?	Specific labels and some reports may not display properly with unsupported browsers.

What components/modules will need to be considered for installation?	If the customer elects to purchase the standard data import service, we utilize SFTP to regularly transfer data.
What are the programming language(s) and versions of the client?	Oracle APEX 3.2.0 Ruby 2.1.1 Rails 4.1.1
What type of patient data [or other confidential data] is stored on your system? Please provide specific listing of data requirements.	Copy of current VQI Data Field Definitions is available upon request.
What is the database type?	Oracle Version 11G Mongo 4.6.4
How long is this data maintained?	Data is maintained indefinitely or until mutually agreed to by both parties in the M2S Data Management Services Agreement and the applicable PSO Service Agreement(s).
Is any of this data used by your company (i.e., for benchmarking or supplied to other organizations/companies for any reason)?	No, our company does not use your institution's data for any other purpose than is mutually agreed to by both parties in the M2S Data Management Services Agreement and the applicable PSO Service Agreement(s), without your prior consent.

Access Information	
How are accounts managed?	User account management is controlled at the local level by a designated database manager at the site. M2S creates the database manager's account upon initial set-up. The local database manager is responsible for maintaining appropriate data access permissions and account terminations for the Institution.
What are the password specifics of the application?	New users are forced to change their password upon first login into the application and have the option to change their password at any time thereafter. Passwords must be eight characters in length and include at least one alpha, numeric, and special character.

	Password changes are forced every 180 days and users may not re-use the same password for at least 5 iterations. Users are locked out after 5 consecutive unsuccessful login attempts. Users must contact their local Database Manager or M2S PATHWAYS Support to unlock the account.
Can the application be set to automatically log a user off the application after a predefined period of inactivity?	Yes. Users are automatically logged off after 15 minutes of inactivity.
Can access be defined based upon the user's job role? (Role-based Access Controls (RBAC))?	Yes. Users are assigned a role within the system that limits the privileges and permissions available to that user. There are 3 individual user roles for each user. They are "Hospital Manager", "Physician", and "Other" and each role has a corresponding set of permissions assigned to each. Definitions of roles and available privileges are outlined in the M2S PATHWAYS User Manual.
Can the application support the removal of a user's access privileges without requiring deletion of the user account?	Yes. The Hospital Database Manager at each institution is responsible for granting access as well as removing a user's ability to access the system. Making a user "inactive" will take away the individual's ability to log in while still maintaining their user account within the database.

Audit Capabilities	
Is audit log tracking a feature available in the current version of this software application?	Yes.
What information can the audit logging capture?	Access to PATHWAYS and patient data views as well as modifications, deletions, and additions to the PATHWAYS data is recorded.
Are audit log reports available for the current version of this software application?	Audit log reports are not available within the application, but can be downloaded in csv format by an M2S administrator and provided upon request.

Security	
Does your company have a formal IT Security team and incident response program?	Yes.
Does your company have an accredited third party perform security audits of your security program?	Yes. A letter of certification which provides details of the audit is available upon request.
Does the application follow HIPAA and HITECH regulations?	Yes. M2S applies administrative, technological, and physical safeguards to meet these regulations.
Describe your Intrusion Detection Systems (IDS) and/or your Intrusion Prevention System (IPS).	We currently utilize Cisco ASA firewalls with built in IDS functionality. These firewalls have current Cisco Smartnet agreements and the firmware is kept up to date according to our protocols.
Do vendor support personnel have specific roles and accesses that control access to ePHI?	Yes. Only trained M2S and SVS PSO personnel who require access to perform their job functions are given access to the application.
Does organization/work group maintain secure or locked facility and/or rooms or areas where information resides or is being stored to reduce tampering or theft of ePHI?	Yes. Both server locations require a key card to enter the facility, and a higher level of access is required to enter the server room. These server rooms use advanced cooling units to keep servers operating at optimal temperatures, inert gas systems for fire suppression, and alarms to sound if any of the environmental parameters fall outside the peak performance levels for operation. Physical access to IT and information hosting facilities where information is stored is restricted based on role of employee, and access is granted only after approval and authorization by applicable facility manager.
Does M2S provide training to ensure that M2S employees understand and adhere to security protocols that ensure the integrity and confidentiality of electronic information?	All employees are trained to HIPAA regulations and company security policies.
What is M2S' process for handling a security breach?	The M2S Incident Response Plan is specified within the BAA.

Configuration Management and Change Control	
What are the internet bandwidth requirements for running the application?	T1 or better Internet connection is recommended for optimal user experience.
Are updates to application software and/or the operating system controlled by a mutual agreement between the support vendor and the application owner?	No. The application is web-based and thus cannot permit partial upgrades.
Do you provide documentation for guidance on establishing and managing security controls such as user access and auditing?	Yes. Documentation and training is provided to the designated Data Managers at the facility.
Does the application encrypt data before sending it over the Internet or an open network? Is data encrypted at rest?	Yes. 256-bit SSL encryption is used for any data transfers and any data at rest utilizes EMC Security Suite.
Please describe your proposed back-up, archive and restore strategy.	Full database backups occur nightly and backup tapes are rotated offsite. A standby database server is maintained in a separate building and updated on a regular basis. We utilize the Oracle Data-guard application to ensure that the standby server is ready at all times with up-to-date information. We utilize mongoDB Master-Slave hot backup model, using mongoDB monitoring & ipMonitoring to check the consistence backup process.

Other Capabilities	
Does the application include documentation that explains error or messages to users and system administrators and information on what actions required?	The M2S PATHWAYS User Manual and FAQ are available to explain such messages.
What are the system performance and response time metrics?	M2S shall maintain and support PATHWAYS for the term of the Agreement and will use good faith efforts to maintain 99.95% uptime for the PATHWAYS system. Routine system maintenance and version upgrades will be conducted outside of normal business hours whenever possible. Notifications for system maintenance that requires system downtime will be sent at least 24 hours in advance to the Institution's designated hospital database

	manager. M2S will make reasonable efforts to respond to technical support requests within a commercially reasonable period of time but does not guarantee that a response will be provided within a specific time period. M2S has a goal of responding to requests within 4 hours of an initial report that is received between 8 AM ET through 5 PM ET Monday through Friday, excluding federal holidays.