

PATHWAYS™

CLINICAL DATA PERFORMANCE PLATFORM

Whitepaper: Security of the PATHWAYS™ Platform

A Secure Solution for Clinical Registries

The safety and security issues associated with externally hosted registries can be divided into three categories: data entry and access, data transmission, and data storage. M2S has addressed each of these areas through its PATHWAYS™ platform, in order to provide assurance to participants that their data are being handled safely and securely.

The PATHWAYS™ platform is fully compliant with HIPAA and HITECH, including the Security Rule (45 CFR Part 164 subpart C), which is the Federal regulation under HIPAA that establishes security standards for the protection of electronic protected health information. The system is also compliant with the security requirements of the Patient Safety Rule (42 CFR Part 3.106). All safeguards provided for protected patient health information (PHI) are also applied by M2S to patient safety work product (PSWP). The Patient Safety Rule states that security “requirements must be met at all times and at any location at which the PSO, its workforce members, or its contractors receive, access, or handle patient safety work product. Handling patient safety work product includes its processing, development, use, maintenance, storage, removal, disclosure, transmission, and destruction.”

M2S plays a significant role in ensuring the adequate security of the PSWP as the data management services provider of Patient Safety Organizations, and takes all necessary steps to comply with all requirements. M2S conducts periodic risk analyses of the potential risks and vulnerabilities to PHI and PSWP, and implements security measures sufficient to reduce risks and vulnerabilities based on the findings of the risk assessment. M2S also utilizes a third party vendor to identify any security vulnerabilities, such as code exploits and cross site scripting.

The PATHWAYS web-application has minimal technical requirements. Users must have an internet connection, either wireless or Ethernet, to access our secure website. The current version of Chrome, and Firefox, IE8, IE9, IE10, and IE11 are certified. The reports require Adobe Flash 9.0 or higher

Data Entry and Access

PATHWAYS™ is a web-based registry which stores information directly into a database at a central data warehouse managed and hosted by M2S in its secured data center. Unique username-password combinations authenticate users and permit access only to the appropriate content. M2S passwords require at least eight characters, including one letter, one numeric digit, and one special character. All passwords are stored using a one-way hash encryption process with a custom salt. Temporary passwords are provided to users for initial log-in to the system, and users are required to create their own password upon first log-in. Passwords expire every 180 days and cannot be reused for five generations.

This ensures that the user is the only person who knows his or her password. PATHWAYS™ will also automatically log the user out of his or her session after 15 minutes of inactivity. To protect accounts from malicious attacks, users will be locked out of the system after five consecutive unsuccessful attempts to log-in. The database manager will then need to unlock the account before the user can log-in again.

Data Transmission

While HIPAA and HITECH address the security and privacy of PHI at a policy and procedure level, these regulations do not provide strict parameters for what type of technology to use. M2S utilizes best practices within the industry for data security. Encryption is typically considered a best practice when it comes to protecting sensitive data. PATHWAYS™ utilizes 256-bit SSL encryption protocols when transmitting data, which is the same technology used by online banking and financial institutions, as well as healthcare providers, to protect their customers' personal information. PATHWAYS™ users do not interface directly with the database server, but rather connect to the registry through a separate front end server. PATHWAYS™ protects PHI by preventing the browser from caching sensitive data. Furthermore, PATHWAYS™ does not require ActiveX or Java plug-ins to run, and never writes PHI to the user's computer. Storage of all identifiable PHI data is encrypted at rest as well on all backups executed. Encryption keys are secured and have strict policy controls restricting the individuals within M2S that are permitted to access them.

Data Storage

The database in which PATHWAYS™ stores data has achieved a C2 rating by the Department of Defense's Trusted Computer System Evaluation Criteria (or "Orange Book"). This rating is given to database systems that provide controlled discretionary access, which means that access to certain data can be restricted based on the identity of the user. M2S has also taken measures to physically separate PSWP from non-PSWP where possible. To address the issue of data disposal, M2S has a written policy for media sanitation that follows the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (NIST Special Publication 800-88).

The entire PATHWAYS™ registry architecture has been replicated to a separate M2S operated data center and the registry data is backed up every night to this second database. Both locations require a key card to enter the facility, and a higher level of access is required to enter the server room. These data centers operate with 24 hour video surveillance and use advanced cooling units to keep systems 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. Data recovery procedures are tested annually to ensure that all of the PATHWAYS™ data is safe and secure.

Summary

An externally hosted, web-based registry with centralized data storage such as PATHWAYS™ provides stakeholders with the most secure and robust solution to the challenges associated with registry creation and data sharing. Users can access registries on this platform from any computer with internet access, and can enter data, submit records, locate existing records, and generate reports without storing any protected health information locally on their computer. The hosting entity can design the registry to proactively ensure that the data being submitted is clean, complete, and consistent, thus enabling pooling of quality data among multiple participating institutions. The participating institutions are not required to install and maintain the registry systems and are not reliant on support from their IT departments.

Rev E June 2016