

CLINICAL DATA PATHWAYS REGISTRY SECURITY

An externally hosted, web-based registry with centralized data storage provides the best and most cost-effective solution to the challenges associated with registry creation and data sharing. Users can access such a registry 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 therefore not reliant upon assistance from their IT departments.

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 Clinical Data Pathways registry, in order to provide assurance to participants that their data are being handled in a safe and secure manner. M2S's Clinical Data Pathways system 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 protections to protected patient health information (PHI) referenced from here forward also apply 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 recognizes that it plays a significant role in ensuring the adequate security of the PSWP as the data management services provider of the Society for Vascular Surgery® Patient Safety Organization (SVS PSO), and has taken deliberate actions to ensure compliance 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 3rd party vendor for identifying any security vulnerabilities, such as code exploits and cross site scripting.

Safety and Security Issues Related to Data Entry and Access

Access to any web-based registry must only be granted to registered users possessing a unique username and password combination. Password strength is a critical consideration, in that each additional degree of password complexity has a significant impact on decreasing the likelihood that the password may be compromised by malicious activity. Further, in accordance with 45 CFR Part 164.312, only the user is permitted to know his or her username-password combination. Therefore, the registry interface must provide the user with a mechanism for changing his or her password, and all passwords must be stored in an encrypted format so that even the registry vendor cannot identify the passwords. It is a best practice to force a periodic password change by users, and to prevent the re-use of passwords for a specified number of generations.

In addition to providing user authentication and access to the registry, the unique username-password combination should also indicate the user's identity to the registry system. A complete registry authentication protocol would also identify the user's institution, the assigned role of the user (e.g. physician, data entry clerk, administrator, etc.), the sections of data entry and reporting that the user may access, and whether or not the user has the permission to submit new data to the registry.

Additionally, a user may need the ability to recall a record from the database so that additional information can be appropriately linked. The user's permissions should strictly govern what content, if any, a user has the ability to recall. Not only should the extent of each user's permissions be determined by their role, but once a user does have access, their critical actions in the system should be tracked in a comprehensive audit log, which further contributes to the integrity of the data.

The registry system should also enforce a session timeout, whereby the user is automatically logged out of the registry after a defined period of inactivity. This feature is extremely important in a web-based registry to prevent unauthorized access to the data, should an authorized user forget to properly log out of his or her session.

Clinical Data Pathways is a web-based registry which stores information directly into a database at a central data warehouse managed by M2S. 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 they are required to create their own password upon their 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. Clinical Data 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.

Safety and Security Issues Related to Data Transmission

The safe electronic transmission of PHI between the registry user's computer and the registry vendor's database requires very stringent security measures. Any web-based registry must employ cryptographic protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to encrypt any data that is being transmitted over the Internet. This prevents unauthorized parties from eavesdropping, tampering with, or sidejacking the information being sent. A secure website can be identified by an "https" prefix, as opposed to a regular "http" prefix, and also by the presence of a small "closed lock" icon somewhere in the browser window (see Figure 1). Most https websites can also be configured to never store any information within the web browser's cache on the client's computer. This is an additional benefit, as it prevents unauthorized users from accessing previously viewed pages in the browser's history.

The interaction between the registry application and the user's computer is also an important security concern. A true web-based application will not require the user to download any software or rely upon ActiveX controls to run. The installation of a Java plug-in should not be required, either. Reliance upon these add-ons can be a hindrance to smooth performance by limiting the number of computers from which the application can be accessed. More importantly, a true web-based registry application will at no point write PHI to the hard drive of the user's computer.

Clinical Data Pathways utilizes 256-bit SSL encryption protocols, which is the same technology used by online banking and financial institutions, as well as healthcare providers, to protect their customers' personal information. M2S registry users do not interface directly with the database server, but rather connect to the registry through a separate server, or "proxy" server (see Figure 2). This proxy server filters all communication between the clients and the database and prevents unauthorized users from accessing the registry data. Communication from authorized users is relayed by the proxy server to the database through M2S's internal firewall. Registry data is never stored on the proxy server, which greatly reduces the possibility for data to be lost, stolen, or accessed by an unauthorized party. Clinical Data Pathways

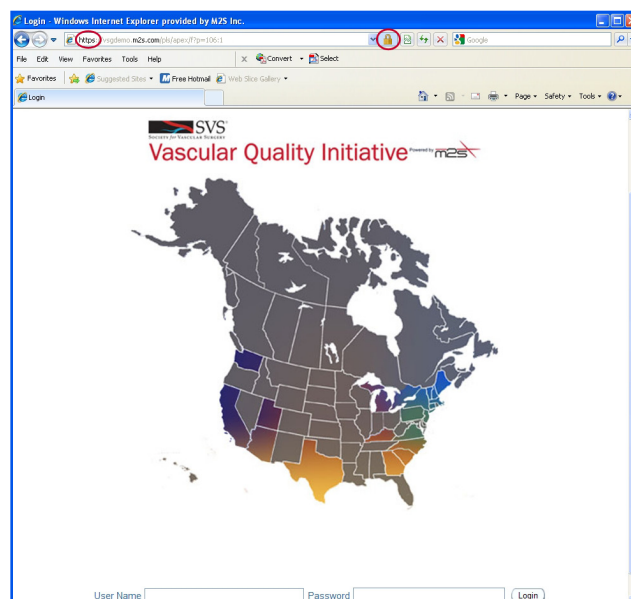


FIGURE 1 Login webpage for data entry. Note the "https" prefix in the URL and the "closed lock" icon, both indicating that this is a secure website.

protects PHI by preventing the browser from caching sensitive data. Furthermore, Clinical Data Pathways does not require ActiveX or Java plug-ins to run, and never writes PHI to the user's computer.

Safety and Security Issues Related to Data Storage

Once registry data is entered by a user and transmitted to the registry database, it must be stored in a safe and secure manner, while still remaining available to the users for recall and reporting. The database hardware should be robust, scalable, and stable. Registry data should also be physically segregated from all other data stored by the registry vendor, and the storage of the registry data on the database must be organized in a way as to prevent the comingling of PHI and clinical data. Most databases are fully relational and link tables of information by a primary key. A registry vendor should store PHI data and clinical information in separate tables, linked by an identifier that is not related to any of the PHI being stored. This provides added security, allowing users to conduct clinical research with de-identified datasets.

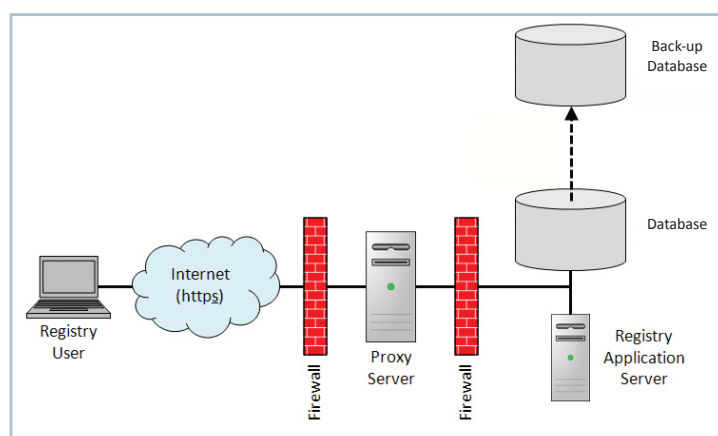


FIGURE 2 Schematic of the registry architecture used by M2S. Note the use of firewalls and proxy server to protect the data.

The appropriate physical location and surroundings of the registry database are critical to the safety and security of the registry data. The database should be located behind a firewall designed to filter incoming and outgoing communications and to prevent access from unauthorized users. Physical access to the server hosting the database should also be restricted. It is important that the registry server room have appropriate environmental controls and a fire suppression system that does not use water. The registry vendor must adhere to a strict schedule of routine maintenance and testing of these systems. An often overlooked, but significant security risk to consider is the destruction or disposal of PHI when its useful life is over.

Finally, the registry vendor must have implemented plans for business continuity and disaster recovery. Regular backing up of the data to a separate database located off-site provides one means of recovering the data in the unlikely event of a disaster at the primary site. Clear fail-over/fail-back and data recovery procedures must be documented, and periodic testing of these procedures must be conducted.

The database in which Clinical Data 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. PHI is stored in a separate table from clinical information and linked via unique identifiers, limiting access to private information by specifically authorized persons only. M2S has also taken measures to physically separate PSWP from non-PSWP where possible, and to make PSWP distinguishable where a physical separation is not feasible. 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 Clinical Data Pathways registry architecture has been replicated to a separate collocation site, 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 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. Fail-over/fail-back and data recovery procedures are tested annually to ensure that all of the registry data is safe and secure.



About Clinical Data Pathways

Clinical Data Pathways is a secure, web-based quality improvement platform that allows physicians, clinical researchers, and institutions to understand and improve patient outcomes by allowing for efficient data collection, aggregation, and analysis of procedure data. It also delivers real-time, anonymous, benchmarked reports of major outcomes and processes of care. Clinical Data Pathways offers the opportunity for long-term outcomes assessment in an effort to improve patient care, enhance clinical quality, and reduce costs, while providing the user with ownership and control over their data.

About M2S

M2S provides medical image and data management services designed to improve patient outcomes through clinical data registries, advanced radiographic image analysis, and aortic device clinical trials. In the field of imaging, M2S has pioneered advanced 3D imaging and data management services for vascular surgery through accurate and efficient pre- and post-operative treatment planning and long-term patient surveillance tools, utilizing its PEMS® (Patient Evaluation and Management System) and Preview® treatment planning software. M2S is an ISO 13485:2003 certified company based in West Lebanon, NH.