sysmex | Lighting the way with diagnostics

WHITE PAPER

Caresphere™ Workflow Solution (WS) Security, Fundamentals and Ideologies

www.sysmex.com/us

The Global Security Landscape Is Continuously Evolving

Prepare for tomorrow's attacks today

The facts:

- Cyberattacks are increasing by more than 320% annually.[1]
- Over 16 million patient health records were breached in 2016.[1]
- Healthcare suffered two to three times more cyberattacks in 2019 than the average amount for other industries.[2]

Measures that protect your patient health records today might not work anymore. Investing in the latest technology solutions now will not ensure your health information is protected from a future attack. You and your patients will not feel secure if protected health information (PHI) isn't protected. Effective and efficient software solutions are not enough. A security framework that grows and adapts to the ever-changing world of cybersecurity must be built into the foundation of your software solution.

From design to deployment, Caresphere WS implements and embodies industry-trusted security pillars, fundamentals and ideologies

As a robust, enterprise-wide and cloud-hosted solution, one of the fundamental foci of Caresphere WS is keeping patient health information secure. To achieve this, Caresphere WS is utilizing the HITRUST CSF® security framework (based on NIST & ISO 27001:27002 and HIPAA/HITECH) to govern Caresphere WS. This ensures the platform's security is assessed, monitored and managed from end-to-end. The HITRUST security framework was selected for its acceptance and prevalence in the healthcare industry, and ability to prescribe, refine and assess an environment's cybersecurity strategy.

Designed with security in mind

Caresphere WS design and development embody the "security as code" culture. Security is an integral part of development, using industry-accepted style guides, automated security checks, monitoring and code reviews.

To effectively isolate and quarantine potential threats, Caresphere WS employs a modular design. Security-focused services are leveraged to enable intrusion detection, protection, and repair. Customized alerts are utilized for quick investigations, behavior monitoring, and responses. Encryption key management decreases administrative overhead and provides customized alerts for quick inquiries and responses.

Secure infrastructure in the cloud

Caresphere WS is housed in a secure, HIPAA-compliant cloud platform.

Caresphere WS in a cloud platform gives you a better experience in support, performance and security - it allows connectivity to your directory services for password authentication and can leverage advanced security services typically not offered in on-premise servers as well as protects against the following major security concerns:

- SQL-injection attacks
- Cross-site scripting attacks (XSS attacks)
- Brute-force HTTP flood attacks
- Attacks from unknown IP addresses

Caresphere WS automates the following:

- Performing and reviewing audits on services, activities and environment changes as well as managing alerts regarding any security gaps.
- Assessing and identifying security gaps and vulnerabilities across the operating system, application and environment.
- Continuously monitoring for malicious or unauthorized behavior to help protect all accounts and workloads from unusual Application Programming Interface (API) calls, unauthorized deployments, compromised instances or reconnaissance by attackers.
- Retaining detailed logging records of transactions and events.

Caresphere WS is designed to perform automatic backups and ensure snapshots are readily available in the event of a disaster, so you can restore your environment with little to no disruption to your day-to-day processes.

Maintaining operational security

Caresphere WS protects your data and environment in day-to-day operations:

End-User Authentication:
Integration with customer directory service allows the customer to control the identity and access of users logging into the application.

Data Encryption:
Caresphere WS employs end-to-end Department of Defense standard FIPS 140-2-compliant encryption in motion and at rest.

Inter-Application Authentication:
Machine-to-Machine (M2M) authentication tokens are exchanged regularly to automate and secure communication between various services within the bounds of the application infrastructure.

Data Privacy:
Protected Health Information data is masked by default upon implementing Caresphere WS.

Internet of Things (IoT) Services:
Caresphere WS and Sysmex Edge Interface Concentrator communications are authenticated periodically to protect against threats and keep data flow secure.

Caresphere WS continuously listens and is vigilant to detect and prevent potential threats:

Supporting the Environment:
Advanced end-point protection service provides anti-virus, anti-spyware, anti-malware; protection from ransomware; and abnormal behavior monitoring capability within the Caresphere WS environment.

Performance Monitoring and Ongoing Protection:
Monitoring, analytics and reporting is provided for the Caresphere WS environment to detect attacks today and continually prepare for future threats.

Fact citations in content

1 CynergisTek Redspin "Breach Report 2016: Protected Health Information (PHI)" published 2017

2 Source: https://cybersecurityventures.com/15-cybersecurity-statistics-to-diagnose-the-ailing-healthcare-industry/

FAQs

Q. Is patient health information data transmitted to external end-points?

A. Yes, PHI is transmitted from one facility to another over the internet, specifically between the Sysmex Edge Interface Concentrator and the Caresphere WS application.

Q. Are subcontractors involved in the services performed by the vendors?

A. No.

Q. Do audit logs capture both system data and user activity in the system?

A. Yes, Caresphere WS includes a user activity log and audit trail functionality to capture activity throughout the system as it relates to user actions and sample activity.

Q. Are there different types of authorization levels for users?

A. Yes, Caresphere WS uses three standard user roles:

- General Lab User
- Laboratory System Administrator
- Sysmex Service User

Q. Will customers be able to customize or manage user authorization levels?

A. Yes, within the user management feature of Caresphere WS, lab administrators are able to further configure each user's permission level into four subsets based on their needs and responsibilities (i.e., IT roles, management, bench technologist).

Q. Will we have downtime when the system is updated?

A. Sysmex has worked hard to minimize the impact of downtime for laboratorians. Caresphere WS is designed to be resilient and efficient and most activities do not require downtime. Any activity requiring downtime will be communicated and short in duration. Activities that may require downtime include database changes and major application version upgrades. These activities will be scheduled and automated to minimize impact and return to service as quickly as possible.

Q. Does Caresphere WS support integration with directory services?

A. Yes, directory services for use of Caresphere WS are mandatory. Caresphere WS was validated with Active Directory/LDAP, the most commonly used directory service. Through Auth0™ integration with the following authentication protocols are supported::

Supported

- SAML
- Open ID Connect
- Google G Suite
- Microsoft Azure AD
- ADFS
- Active Directory/LDAP
- Ping Federate

Q. Does the solution utilize a built-in authentication and authorization system?

A. Caresphere WS supports authentication through your directory services integration with Auth0 authentication platform, using the previously described SAML 2.0 and LDAPS.

Q. Do you have formally documented policies and procedures on your security protocols?

A. Caresphere WS has adopted the HITRUST security framework as its information security program. HITRUST requires policies and procedures for 19 security facets that are all formally documented. HITRUST requires a robust and thorough incident management program to be established and continually tested for capability to ensure timely and effective responses to security incidents related to Caresphere WS.

Q. Are interconnection security agreements documented (e.g., interface characteristics, security requirements, data types transmitted)?

A. As part of your implementation, you will be provided with the Sysmex interface specifications and IT guidelines and settings to implement accordingly.

Authentication Service

FAQs Continued

Q. Does this information system interface with any other information systems?

A. Caresphere WS interfaces with our Sysmex Edge Interface Concentrator, which interfaces with your Sysmex hematology and your Laboratory Information System (LIS). *(Figure 1)*

Q. Does your organization do penetration testing on internal networks?

A. As part of security best practices, penetration testing is conducted annually by a third party; this happens in Sysmex internal environments. Additional application penetration testing is regularly conducted as a requirement of Sysmex's software development life cycle process.

Q. Is the flow of sensitive information secured between interconnected systems (e.g., firewall rule sets, iptables, proxies, encrypted tunnels)?

A. Yes, Caresphere WS employs end-to-end encryption of sensitive information through TLS V1.2 and FIPS 140-2 compliant encryption techniques. A firewall is in place to protect from proxies, unknown IP addresses and other attacks.

Q. Does Caresphere WS allow wireless access?

A. The Sysmex Edge Interface Concentrator (E-IC) is installed in your network and requires a network connection that has access to the internet, your instruments and your lab information system LIS *(Figure 1)*. The method of E-IC connection is chosen by the customer. Users will access Caresphere WS by the method chosen by the customer.

Q. Are there components of the solution that can be hosted by the vendor of a third party?

A. There are third party components that provide authentications, monitoring and end-point protection services that have been implemented and validated to work with and support Caresphere WS.

Q. Is there publicly accessible information?

A. No, access to Caresphere WS is permitted by authorized IP addresses. Any data contained within the system requires authentication to access.

Q. Is basic security awareness training performed for all Sysmex personnel as part of an onboarding process?

A. Yes, Caresphere WS is adopting the HITRUST framework, which requires training on all 19 domain procedures. Additionally, Sysmex requires an annual IT security awareness training.

HITRUST
CSF Certified

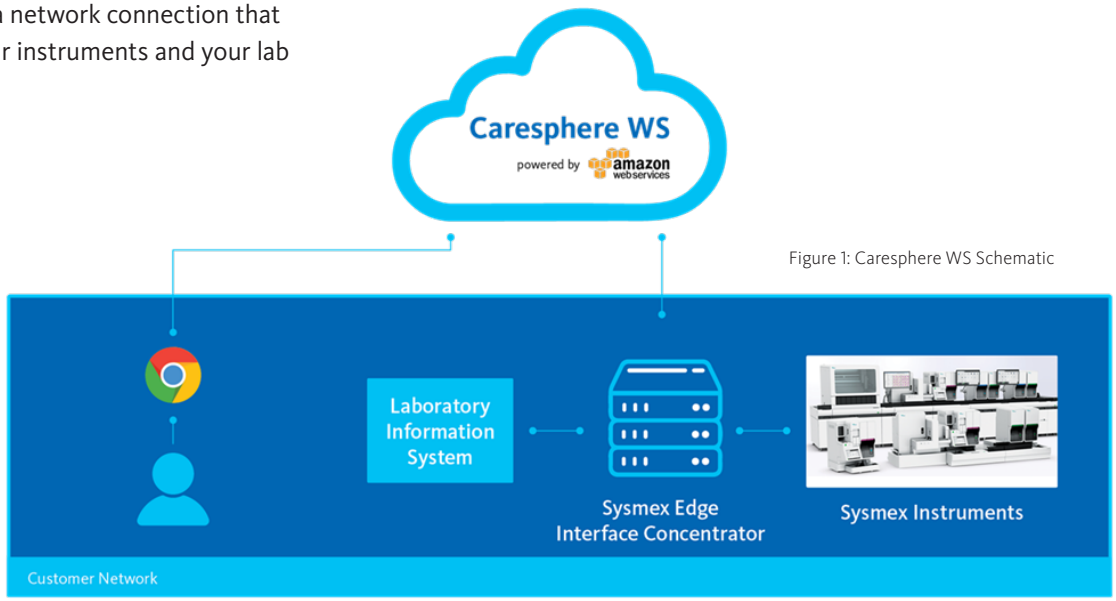

Figure 1: Caresphere WS Schematic

Q. Does this solution provide the capability to generate customizable audit reports?

A. Yes, Caresphere WS includes a user activity log and audit trail functionality. The data can be filtered, printed and exported. *(Figure 2)*

Q. Are the audit logs time-stamped (date and time)?

A. Yes, Caresphere WS will collect and display date and time attributes for both the user activity log and audit trail.

Q. Do you have formally documented policies and procedures for a contingency plan?

A. Yes, HITRUST requires policies and procedures for Business Continuity and Disaster Recovery including backup and restoration. HITRUST also requires a full incident management program to be established via policies and procedures, and tested for capability in the event of a security incident or breach.

Q. Does the information system use multifactor authentication for privileged or non-privileged access (tokens, passwords, biometrics, etc)?

A. All authentication is controlled through a provider that has been fully implemented and validated with Caresphere WS to connect customer directory services.

Q. Will the solution require Windows® server components? If so, what are the specifications?

A. No.

Q. Will the solution require a desktop component? If so, what are the specifications?

A. No, the solution is browser-based. We recommend Google Chrome™ for the best user experience.

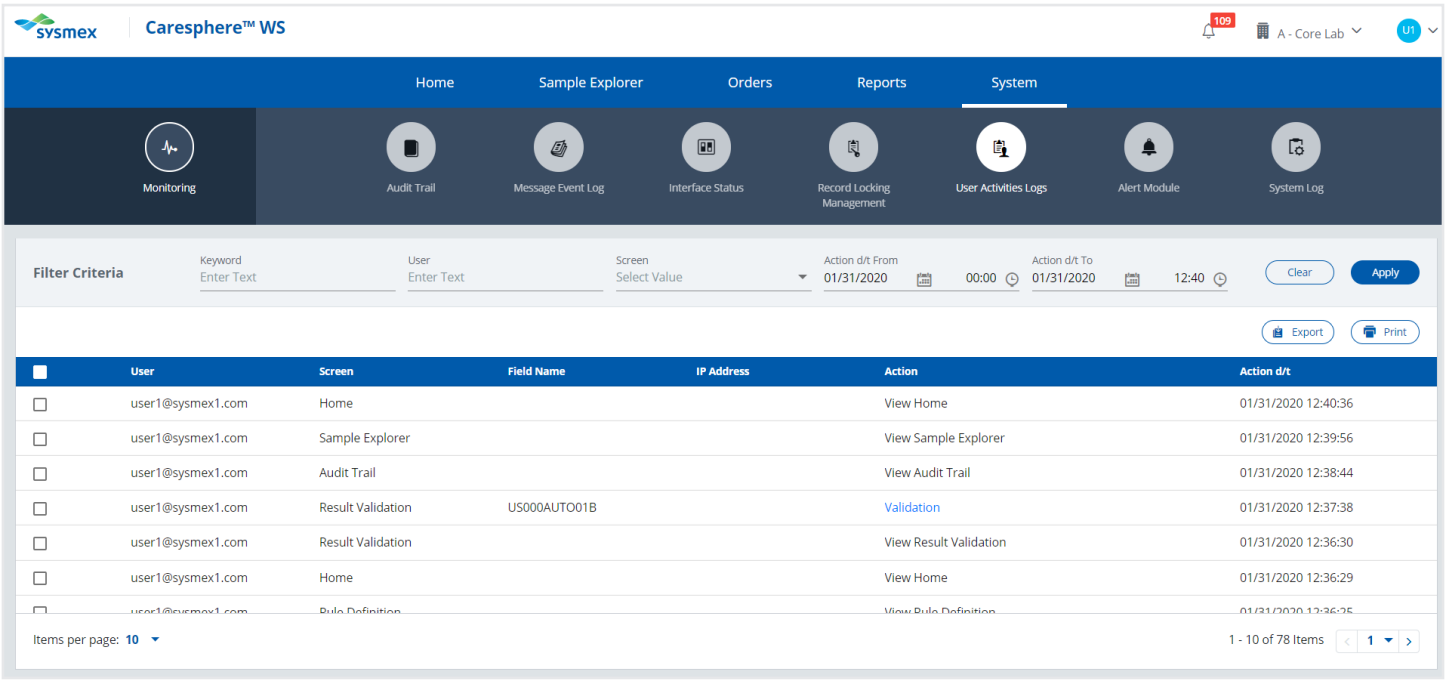

Figure 2: User Activities Logs

Sysmex America, Inc.
577 Aptakisic Road, Lincolnshire, IL 60069, U.S.A. · Phone +1 800 379-7639 · **www.sysmex.com/us**

Sysmex Canada, Inc.
5700 Explorer Drive Suite 200, Mississauga, ON L4W0C6 Canada · Phone +1 905 366-7900 · **www.sysmex.ca**

MKT-10-1302, Rev. 1, 07/2020