The Studycast System

Secure. Private. Available.

Core Sound Imaging knows when it comes to protection, access, and privacy of medical data, we must prepare for everything, because our clients count on us.

Secure.

Your data is secure with Studycast because we use the industry standard for high quality encryption, 256-bit AES encryption on all data at rest. Studycast transfers data using secure socket layer (SSL) encryption (TLS v1.3 256-bit) and HTTPS. Our servers have 2048-bit Extended Validation (EV) Secure Server Certificates issued by GeoTrust Inc.

Access security to Studycast is role-based and permission configurable, allowing our clients to set permissions to meet the security guidelines of their facility. User roles (physician, staff, etc.) can be customized, providing control over what a user can see and do by a single point of contact desired by your facility.

Private.

Security designed to protect your data and meet your organizations compliance requirements

Core Sound Imaging's Studycast system meets or exceeds all HIPAA/ PIPEDA privacy requirements. As a registered medical device manufacturer, Core Sound Imaging meets all applicable regulatory requirements. Our ISO 13485 certification and ISMS 27001 system demonstrate our dedication to quality and security.

Protecting our users' data is paramount, and the Studycast team strives to provide the best system and data security by architecting and developing to the most broadly recognized security standards. We employ rigorous measures at both the architectural and operational levels to keep your data safe and secure. The Studycast system infrastructure provides the latest tools to deliver robust security support.

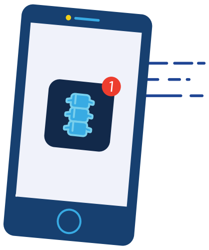
As a cloud provider, our private Tier III+ data center's SOC 2 compliance provides clients with the confidence their imaging workflow solution is adhering to security, availability, data integrity, confidentiality, and privacy best practices. Independent SSAE 16 audits and adherence to our Information Security Management System (ISMS 27001) ensure we are following vital standards.

Security architecture and practices

The Studycast team uses industry-accepted best practices to keep your data safe. Our security approach focuses on security governance, risk management and compliance, including data encryption at rest and in transit, network security, administrative access control, system monitoring, logging, and alerting.

Studycast includes a robust set of security and data protection product features giving you the tools needed to manage all your security challenges.

Available.

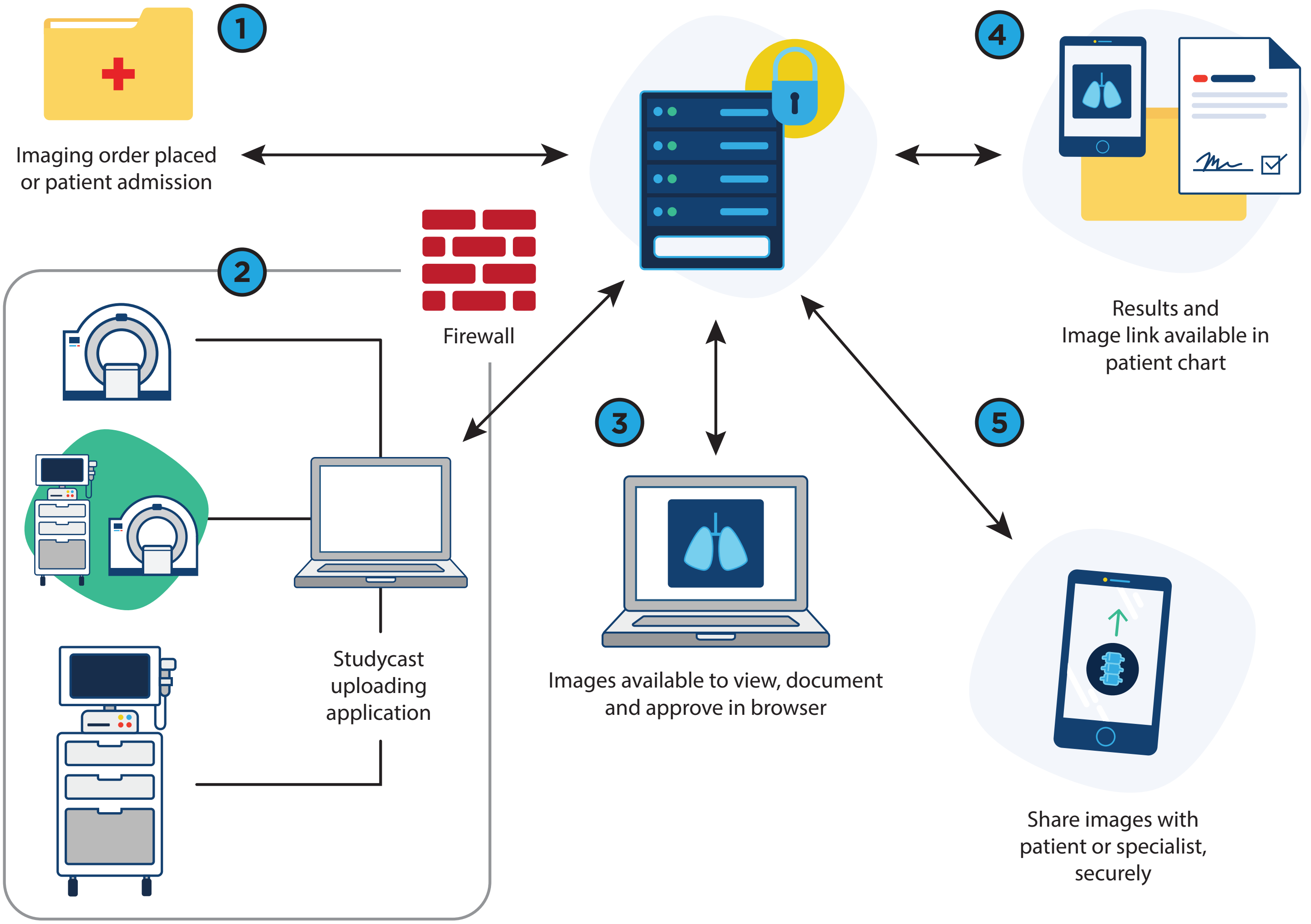


Let's face it, you need to view your images when and where you want. You also need your images connected to your medical record system. Core Sound Imaging has been delivering the Studycast System with greater than 99.9999% uptime for 15 years and counting.

Studycast communicates effectively with other systems to improve efficiencies as well as quality of care by interfacing with many leading EMR vendor APIs and, most importantly, supporting Health Level 7 (HL7) standards. Studycast uses MirthConnect, the leader in vendor agnostic, cross-platform, HL7 engines, to ensure efficient interface solutions are available for our clients. These integrations must be easy to implement and improve your workflow to be effective.

Workflow Simplified

Improving productivity through connections.


1
Imaging order placed or patient admission
2
Firewall
Studycast uploading application
3
Images available to view, document and approve in browser
4
Results and Image link available in patient chart
5
Share images with patient or specialist, securely

1. The Studycast system supports both encounter and orders-based workflows, receiving ORM, ADT or SIU messages and creating a Modality Worklist (MWL).
2. Imaging is then performed on modalities configured to send to a DICOM Store SCP. The DICOM Store SCP is a component of the Studycast uploading application, which receives the study, and securely uploads images and DICOM SR to the Studycast servers.
3. Studycast users, with appropriate permissions can sign into the Studycast application, view images and either create a preliminary report (technologist/sonographer) or approve the exam (physician).
4. Upon approval, the final report can be routed via ORU to the EMR. This ORU message can include a PDF (base-64 encoded) and/or text-based result along with a link to the images. This ORU message can include a base-64 encoded PDF and/or text-based result along with a link to the images.
5. Additionally, study images and/or report can be shared with the patient or a specialist securely with the CoreShare functionality.

Security Details

Policies

Core Sound Imaging is committed to achieving total customer satisfaction through superior customer service, innovation, and constant improvement of its business processes. Our mission is to successfully deliver to customers high-quality, cost-effective products and services reliably.
To fulfill our mission, the policy is to maintain a practical but comprehensive Quality System based on its stated commitment to customer satisfaction and process improvement.

As part of our ISMS/QMS, Core Sound Imaging maintains the following documented procedures/policies:

- Document and record control
- Regulatory requirements
- Information security policy
- Risk assessment and treatment
- Internal audit
- Measurement
- Management
- Mobile devices
- Acceptance
- Asset management
- IT security
- Information classification
- Access control
- Encryption Policy
- Supplier security
- Incident management
- Awareness training
- Media protection
- Personnel security
- Purchasing (system and services acquisition)
- Communication
- Business continuity (contingency/disaster recovery)

Personnel/Awareness

The Information Security Officer at Core Sound Imaging oversees the Information security program and our formal complaint/CAPA system tracks all issues to resolution. Management is made aware of all logged issues. Employees at Core Sound Imaging participate in annual training to review our security policies and are required to acknowledge an understanding of the policy. All employees complete a background check as a condition of employment, as well as sign an NDA. Upon termination, a formal process for discontinuing access is followed.

Security training for employees and contractors includes:

- Annual training
- Social engineering testing
- Phishing testing

Information security roles and responsibilities

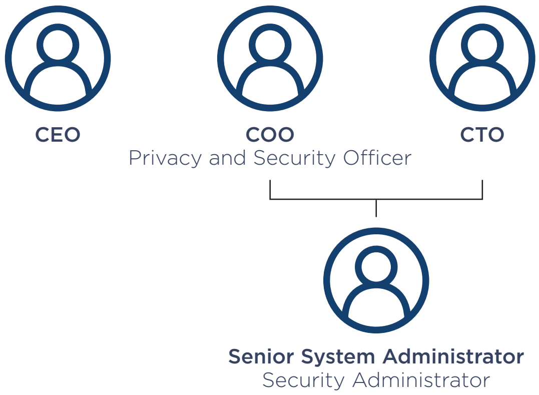


Figure 1 Security Organization Chart

Risk Assessment

Core Sound Imaging performs risk assessments and reviews to identify risks potentially impacting the confidentiality, integrity, and availability of data on our network. Risk assessments identify assets, related vulnerabilities, threats that could exploit vulnerabilities, and the criticality of the risks identified. We have a formal risk treatment process for reducing and controlling risk. The risk assessment is evaluated annually by management to ensure it complies with formal policy as part of our ISMS system following the ISMS 27001 standard.

Information Classification

Core Sound Imaging maintains a formal procedure for the classification of information, which determines encryption and limited access of information based on the classification scheme.

Access Control

Studycast supports role-based permissions and access. All Studycast users, client users and Core Sound Imaging staff, have access granted to the system based on roles. User access and permission level is managed by users with administrative privileges in the client's organization and according to client policies. Within Core Sound Imaging, access is controlled according to our formal Access Control policy.

Studycast administrators control the permissions of all Studycast users associated with a client's account. System Administrators control the security settings and dictate password strength and expiration periods.

Studycast provides robust tools to manage users and groups, streamline authentication using your identity provider, and assign user roles and permissions; ensuring that only the right people can access your organizations data. Studycast access and identity controls include:

- Role-based Access Controls
- Two-Factor Authentication (2FA) Support
- Single Sign-On (SSO) Support
- Account lockout threshold
- Account lockout duration (min)
- Reset account lockout threshold
- Minimum password length
- Enforce password history
- Password strength
- Password expiration
- IP Address filtering

Identification and Authentication

Password strength, password expiration period, lockout attempts, access timeouts and login duration are all configurable in Studycast. Studycast requires users to change issued temporary passwords on first login and all passwords are encrypted using a hash function.

Two-factor authentication (2FA) is available with Studycast providing an extra layer of security using Time-based One-Time Password (TOTP) authentication. 2FA is configurable by the client administrator and can be required, optional, or never required for users on your Studycast account.

Studycast supports Service Provider (SP) initiated Single Sign-ON (SSO) and works with clients' SAML Identify Provider (IdP).

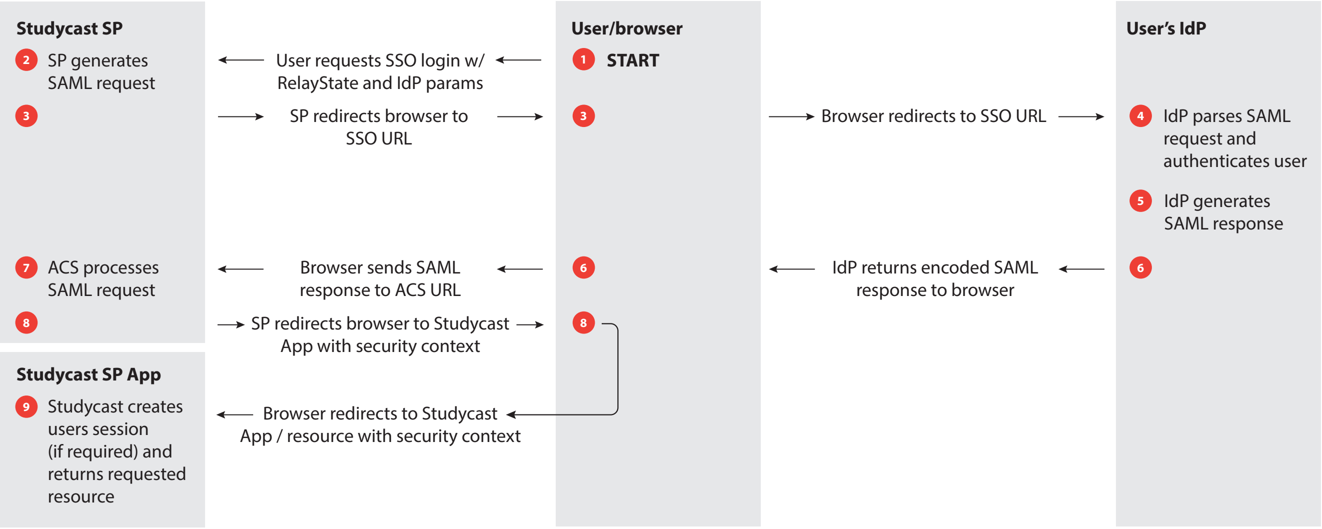

Studycast SP
2 SP generates SAML request
3
7 ACS processes SAML request
8
Studycast SP App
9 Studycast creates users session (if required) and returns requested resource
User requests SSO login w/ RelayState and IdP params
SP redirects browser to SSO URL
Browser sends SAML response to ACS URL
SP redirects browser to Studycast App with security context
Browser redirects to Studycast App / resource with security context
User/browser
1 START
3
6
8
Browser redirects to SSO URL
IdP returns encoded SAML response to browser
User's IdP
4 IdP parses SAML request and authenticates user
5 IdP generates SAML response
6

Figure 2 Studycast SSO Diagram

Physical and Environmental Security

Core Sound Imaging data centers that house data for the Studycast system are independently tested for appropriate physical and environmental security. Periodic data center vulnerability testing is conducted, and results are reviewed with management. SOC 2 reports are available upon request.

All Core Sound Imaging staff providing support and service for the Studycast system are granted access as required to perform their job functions. System access requires approval and is tracked centrally within our organization. Access status changes are implemented immediately.

The Core Sound Imaging offices, where support and service staff are employed, have physical safeguards that include locked doors, surveillance equipment and access cards. Facility recordings are maintained for more than 3 months. Both the primary and secondary Studycast data centers provide alerts regarding access. Visitors must sign in and are always escorted throughout the facilities at our operational facilities. At the data centers, visitor badges are issued as an additional precaution.

The risk assessment completed by Core Sound Imaging, as part of our ISMS, includes an assessment of physical and environmental risks. Employee badges use unique identifiers linking badges to the specific employees and each employee maintains a photograph on file. In the event of a lost or stolen badge, Core Sound Imaging has established policy to mitigate associated risk.

System Communication and Data Protection

Network segmentation is in place to isolate sensitive and critical components of the Studycast system. IDS/IPS is used to detect and prevent unauthorized activity. Alerts regarding security incidents and the responsiveness of our servers are monitored 24/7. We have data loss prevention system to guard against unauthorized access to ePHI for all client data.

Studycast separates all data by client. There are no exceptions to this rule. In fact, in situations where a Reading Physician provides interpretation services to more than one Studycast client, that Reading Physician must have separate login credentials for each client (fast user switching makes this more convenient). At the logical level, Studycast restricts access to data based on user roles and study status. For a study that is assigned to a certain ‘division’ (a client has 1 or more divisions), reading physician group, referring physician group, with a certain status (a study may have one of the following values for status: UPLOADING, NEW, PRELIMINARY, REVIEWED, FINAL) the following access rules apply:

- Client users may only access the study if they have access to the division to which the study is assigned
- Reading physicians may only access studies assigned to a Reading Group to which they belong, and the status of the study is PRELIMINARY or higher
- Referring physicians may only access studies assigned to a Referring Group to which they belong. If the study is not FINAL the Reading physician may only confirm the existence of the study. If the study is FINAL then the Reading physician may also view the report

The Studycast system uses SSL/TLS 1.2 or 1.3 to encrypt data in transit and enable secure data transport, and an AES-256 encryption algorithm utilized to protect data at rest. Manual storage, and rotation of encryption keys are managed by 2-5 people with access, and who formally acknowledge their responsibility to protect and encrypt the keys.

.

System Architecture

Studycast is a web application based on a standard client-server model and Model-View-Controller software architecture. Studycast uses a LAMP solution stack of free and open-source software. Studycast system architecture components include:

- Firewall with fail-over redundancy
- Load balancer with fail-over redundancy
- Web nodes 1-8
- Authentication nodes 1,2
- Production CoreGateway
- Mirth/HL7 server
- Database cluster
  - Master (DB1)
  - Slave (DB2)
  - RDU RepSlave
  - CSI RepSlave
- SQS server
- SQS DB servers

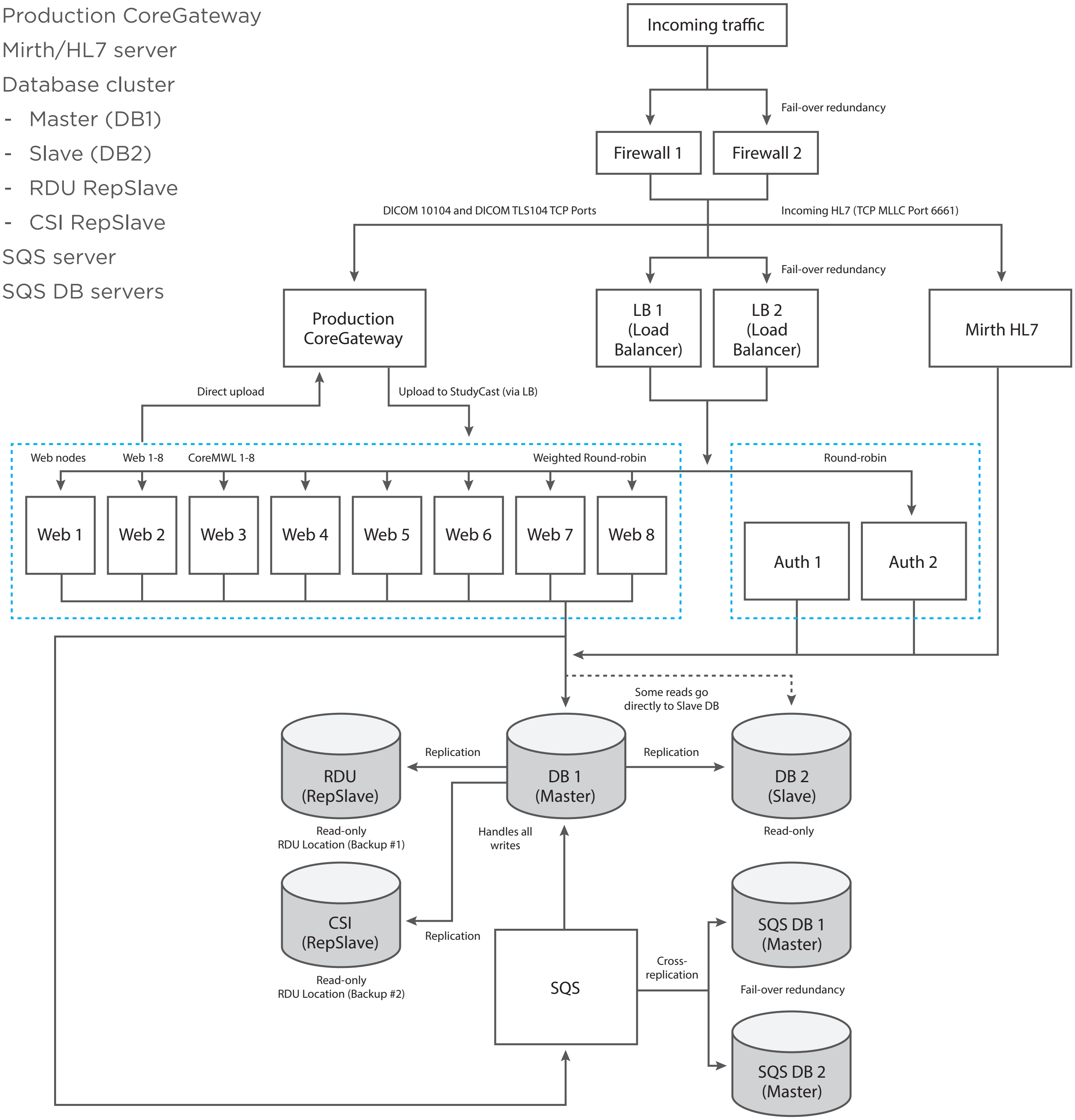


Figure 3: Studycast 6.x System Architecture

Modality Worklist Communication With EMR/RIS

The Studycast Modality Worklist product, CoreMWL, provides users with the ability to retrieve MWL information from a remote scheduling system (EMR/RIS/HIS) and populate corresponding patient/study details on a local modality (see figure 4).

CoreMWL application consists of the following components:

1. CoreMWL Client
2. CoreMWL Server

There is one CoreMWL Server serving CoreMWL Clients.

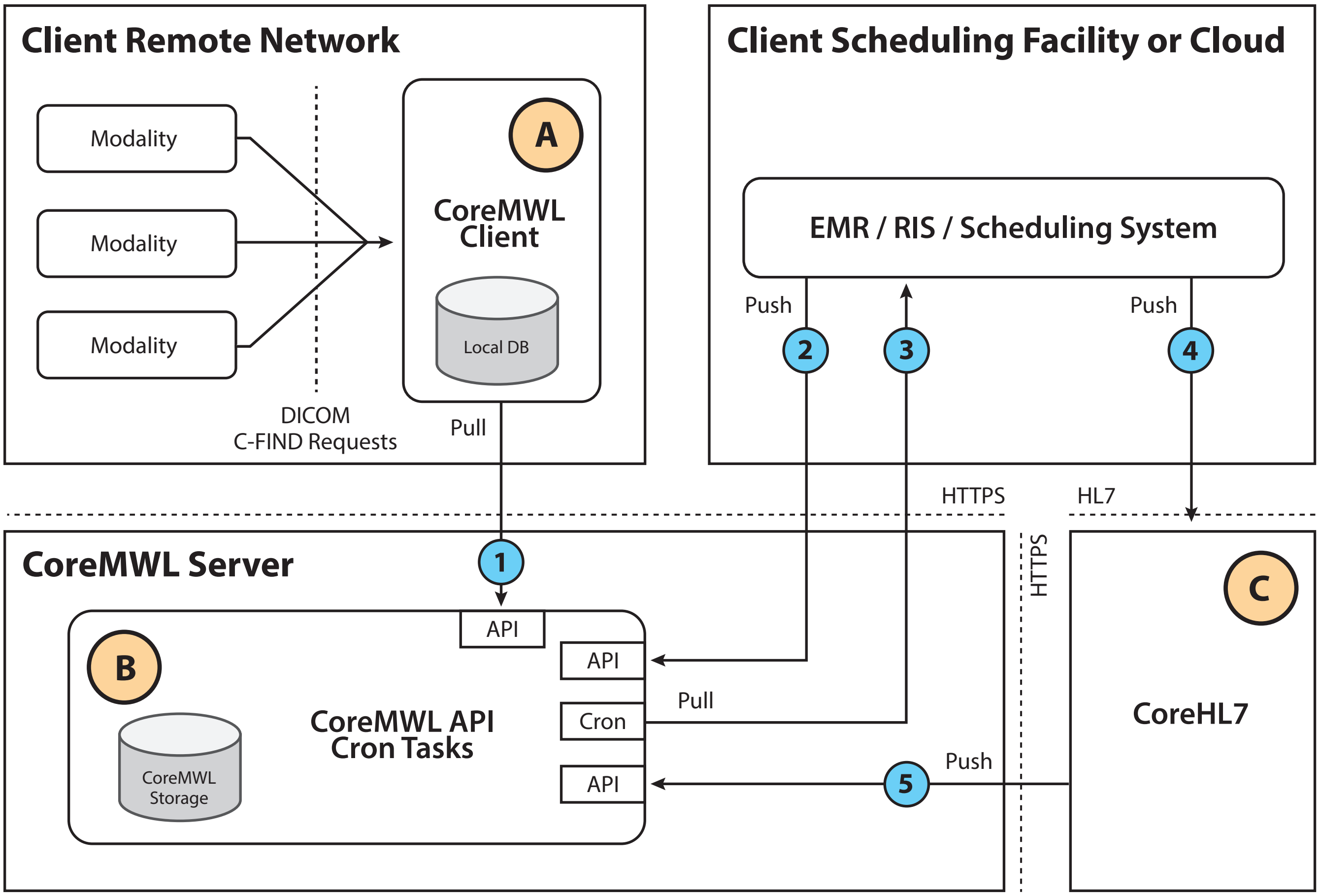


Figure 4 Studycast Integration with an orders interface

A – CoreMWL client (client side)

B – CoreMWL server (Core Sound Imaging)

C – CoreHL7 – receiving/handling HL7 messages and pushing messages to CoreMWL server

studycast®

www.corestudycast.com

5510 Six Forks Road, Suite 200
Raleigh, NC 27609
Office: 919.277.0636

coresound® IMAGING