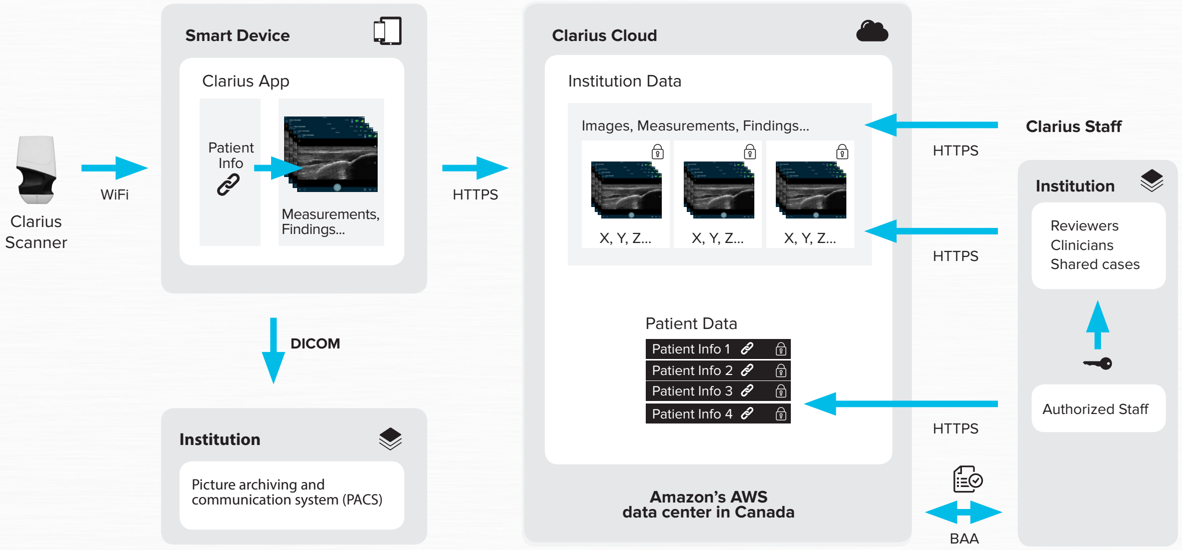
Data Storage and Security

Secure Exam Storage is a Priority

Unlike traditional ultrasound systems that store exams on hard drives and allow users to export or download images to a thumb drive or CD, Clarius manages secure access to images on the Clarius Cloud. The Clarius App, which is on the mobile device used for imaging, only temporarily stores encrypted exams. Patient data is not visible on the mobile device during imaging. Once Internet connectivity is available, stored images are securely transmitted to the Clarius Cloud.



Clarius App

Users can choose to enter patient data on the Clarius App, which is then associated with the images in an encrypted file. The Clarius App temporarily stores the images and patient information in a private, encrypted storage space on the smart device's operating system (OS).

On **Apple devices,** this storage space is encrypted natively by iOS.

On **Android devices,** storage space is segregated from other apps on the device and from the user. Because rooting the device may break this Android-enforced protection, we recommend that Android users do not use rooted devices, and that they enable hard drive encryption.

Once the Clarius App successfully stores the image remotely (ie, to the Clarius Cloud), the patient information is deleted from the device within 30 days.

** Clients who want to automatically store their Clarius Ultrasound Exams on their own Patient Archiving and Communication System (PACS), will be able to select the DICOM option when available. By default, Clarius does not provide encryption in this type of implementation.*

Access to the Cloud

Credentials are required to log into the Clarius App and the Clarius Cloud. Passwords are encrypted and secured using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST.

Clients are allowed to define their own password complexity mechanism when using Clarius Cloud.

Clarius cannot see or retrieve user passwords. Forgotten or lost passwords can be reset through the Forgot Password mechanism.

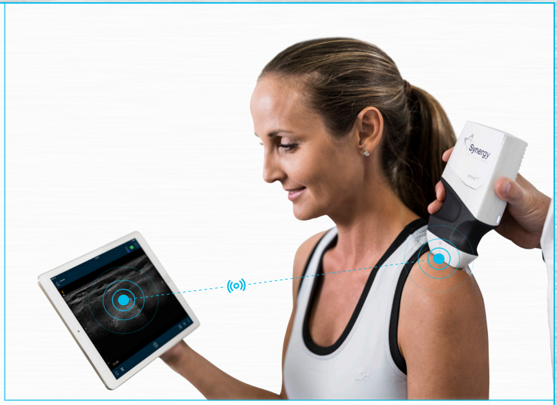
Arthrex®

ePHI in the Cloud

On the Clarius Cloud, patient information and images are stored in separated logical servers. Patient information is stored encrypted in the database server. Images are de-identified before storage. The image file alone does not store any patient information on their records. Clarius does not store ePHI outside the Cloud.

Clarius uses Amazon AWS standard encryption method for storing both patient information and images. In both cases, Amazon uses AES256 for encryption, which is FIPS 140-2 compliant.

NOTE: Images, measurements, and findings can be shared by the exam owners without showing/enabling access to patient data.



Cloud / APP Communication

All communication established with the Clarius Cloud, either from Clarius App or from the user's browser, is encrypted by using at least 256-bit TLS 1.2 encryption across all services. This is the same technology widely used by browsers in secure communications throughout the Internet. The cloud connection is used to pull user data, Clarius Scanner permissions, and settings from the cloud.

NOTE: TLS 1.2 is FIPS 140-2 compliant and uses the following protocols: ECDHE-RSA-AES256-GCM-SHA384

Compliance with HIPAA

Clarius adopts HITRUST CSF (Common Security Framework) as its security framework. The HITRUST CSF Assurance program is a common, standardized methodology to effectively and consistently measure compliance. The CSF integrates requirements from many authoritative sources such as ISO, NIST, PCI, HIPAA and others; it tailors the requirements to a health care organization based on specific organizational, system and regulatory risk factors.

Retention

Clarius stores patient information for 7 years. The system is backed up every hour. These encrypted backups are stored and retained for 1 year.

Physical Storage

All data is stored on the Clarius Cloud, which is stored in data centers located in Amazon's AWS data center in Canada. Clarius does not store patient information outside of the Clarius Cloud.

Monitoring

The Clarius Cloud is continuously monitored (24x7x365) for security and operational purpose. Events traced are stored in a Security Information and Event Management (SIEM) solution hosted by a third party. Actions that may threaten the secure environment or compromise the confidentiality of patient information are recorded and investigated.

Clarius Cloud is monitored by Alert Logic. More information on Alert Logic can be found at www.alertlogic.com.

Logging

Operations involving patient information in the Clarius Cloud are logged and can be reviewed anytime by clients with administrative credentials. Logs cannot be changed or erased prior to the 6-months retention period. Logs can be exported for long-term retention.

Vulnerability Management

The Clarius Cloud regularly undergoes comprehensive internal vulnerability checks to validate the overall security of its system. Clarius uses Tenable technology for regular vulnerability scans (more information at https://www.tenable.com/products/tenable-io).

The security of the Clarius Cloud is also validated by an independent third party (KPMG).

Arthrex®