White Paper

Information Security

by **Luis Araujo**, Manager, Information Security
HITRUST CSF Practitioner, CISSP, CISM, CISA
Clarius Mobile Health

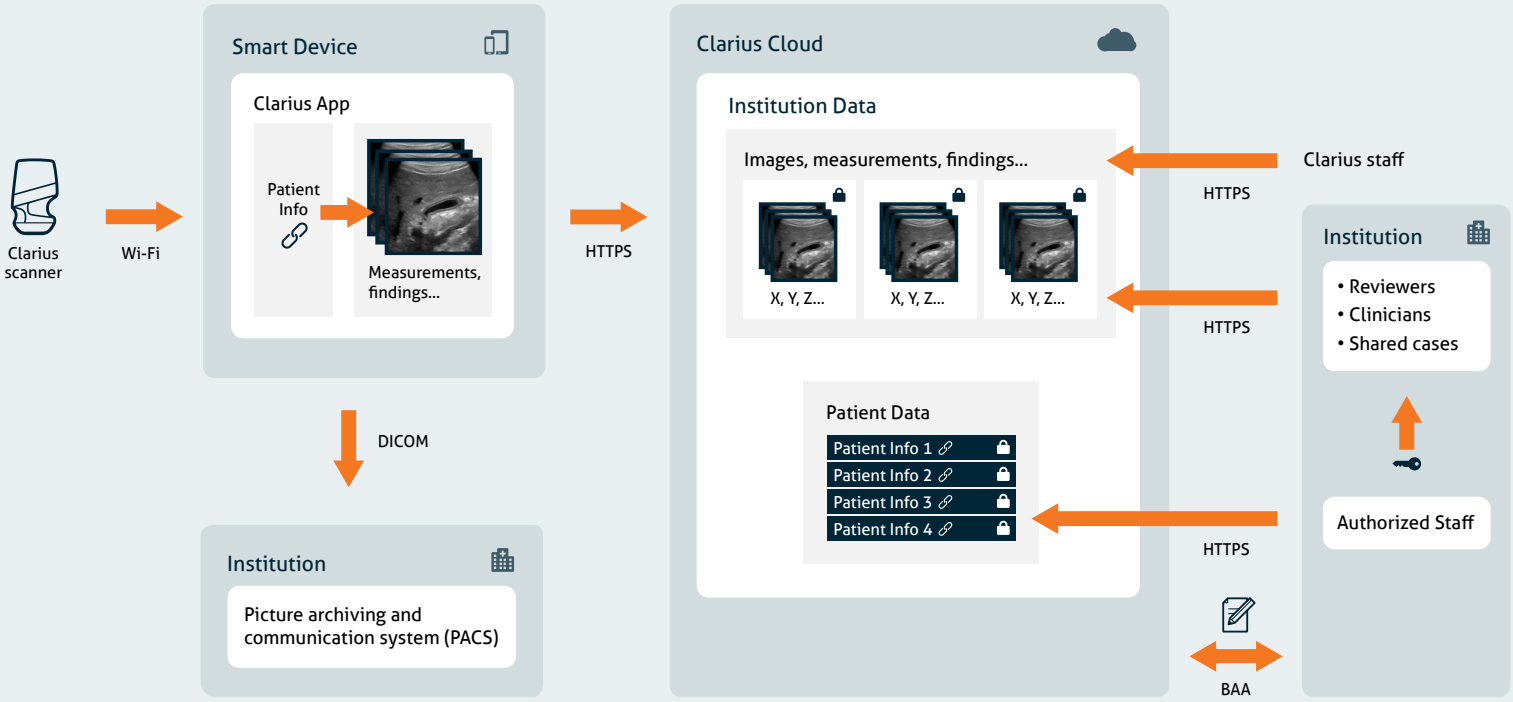
Introduction

The Clarius Scanner is a fully-featured ultra-portable ultrasound device that provides high-quality and cost-effective imaging, while minimizing the limitations of traditional cart-based ultrasound. Clarius develops an ecosystem of data management tools as well as uses traditional storage tools, such as DICOM or exporting to persistent mobile device storage. The solution as a whole is comprised of three main components:

1. Clarius Scanner
2. Clarius App
3. Clarius Cloud

Traditionally, patient data associated with medical devices has been stored within medical facilities. As healthcare technology has advanced and cloud storage become more secure and convenient, alternative storage options are becoming available. Storage outside a medical facility can raise concerns over the security of patient data storage. Clarius takes healthcare data management seriously, and implements strict requirements for security, confidentiality, and privacy according to published standards. The Clarius patient data management infrastructure uses controls and safeguards to protect Electronic Protected Health Information (ePHI) from unauthorized changes and access.

Fig. 1
Clarius security architecture



Clarius Scanner

The Clarius ultrasound scanner is a portable, software-controlled, diagnostic ultrasound system used to acquire and process real-time, high-resolution ultrasound data. The device uses a system of Bluetooth and Wi-Fi-based technology to communicate with existing off-the-shelf tablets and smartphones. Protected Health Information (PHI) is not stored on the scanner at any point of the imaging process.

Wi-Fi Communications

The scanner communicates wirelessly with an App through either an existing local Wi-Fi connection, or more commonly a dedicated Wi-Fi Direct connection.

Wi-Fi Direct

When using Wi-Fi Direct, there is never any WAN or Internet exposure. The mobile device and the scanner have a 1:1 connection. The scanner's Wi-Fi Direct uses WPA2 security and connects with a password provided to the App and user. In most cases, the mobile device can automatically connect to the Wi-Fi Direct network without user intervention, and the password is stored in the mobile operating system's encrypted network settings cache. The Wi-Fi Direct password is randomly generated when the scanner comes out of production, and can be reset or manually set at any time by an authenticated user through the App.

Wi-Fi Routers

Local Wi-Fi networks that support WPA2 can be used to connect through. The user enters the password into the App once, in which it is securely transmitted over Bluetooth for the scanner to connect. The scanner stores passwords encrypted using PBKDF2 with a SHA256 hash to inaccessible persistent storage within the device. At any time, an authenticated user can delete all cached network SSIDs and passwords from the scanner through a connected App.

Real-time Operation

Once a secure connection has been established, all information traveling between the scanner and the App is sent over a TCP socket that is separately encrypted using TLSv1.2.

Bluetooth Communications

Bluetooth is used to negotiate an out-of-band handshake where network information and passwords are communicated. All traffic over Bluetooth is encrypted with both Bluetooth's standard encryption modules as well as an extra layer of AES128 encryption. The AES key is randomized for each new Bluetooth connection and communicated using a public key method built upon RSA256.

Clarius App

The Clarius App runs on Android and iOS mobile devices and is used as an interface for the ultrasound scanner. Preset workflow applications allow the user to control specific aspects of the imaging, such as ultrasound frequencies and depth of imaging. Other controls for data storage allow flexibility on how data is exported.

Users have the option to enter patient information on the App, which is then associated with the images for future storage considerations. The App temporarily stores the images and patient information in a private, encrypted storage space on the mobile device's operating system. On Apple mobile devices this storage space is encrypted natively by iOS, and on Android devices, storage space is segregated from other apps on the device and from the user. As rooting a device may break Android-enforced protection, Clarius recommends that Android users do not use rooted devices, and that they enable encryption of persistent storage.

Once an exam has been performed, there are three possible storage solutions:

1. Clarius Cloud Storage
2. DICOM Store to Existing PACS (Patient Archiving and Communication System)
3. Export to Camera Roll

After examination data has been exported to Clarius Cloud, PACS, or both, all temporary PHI data stored on the mobile device is deleted after 30 days. In the future, this retention policy will be a parameter provided by the institute, with the default set to 30 days.

The Clarius App periodically requires an Internet connection to update security certificates, as well as perform security or feature updates to the App. The user can choose how they connect to the Internet on the mobile device, with common options for Wi-Fi being WPA2 or WPA2 Enterprise if their wireless routing equipment supports the standard.

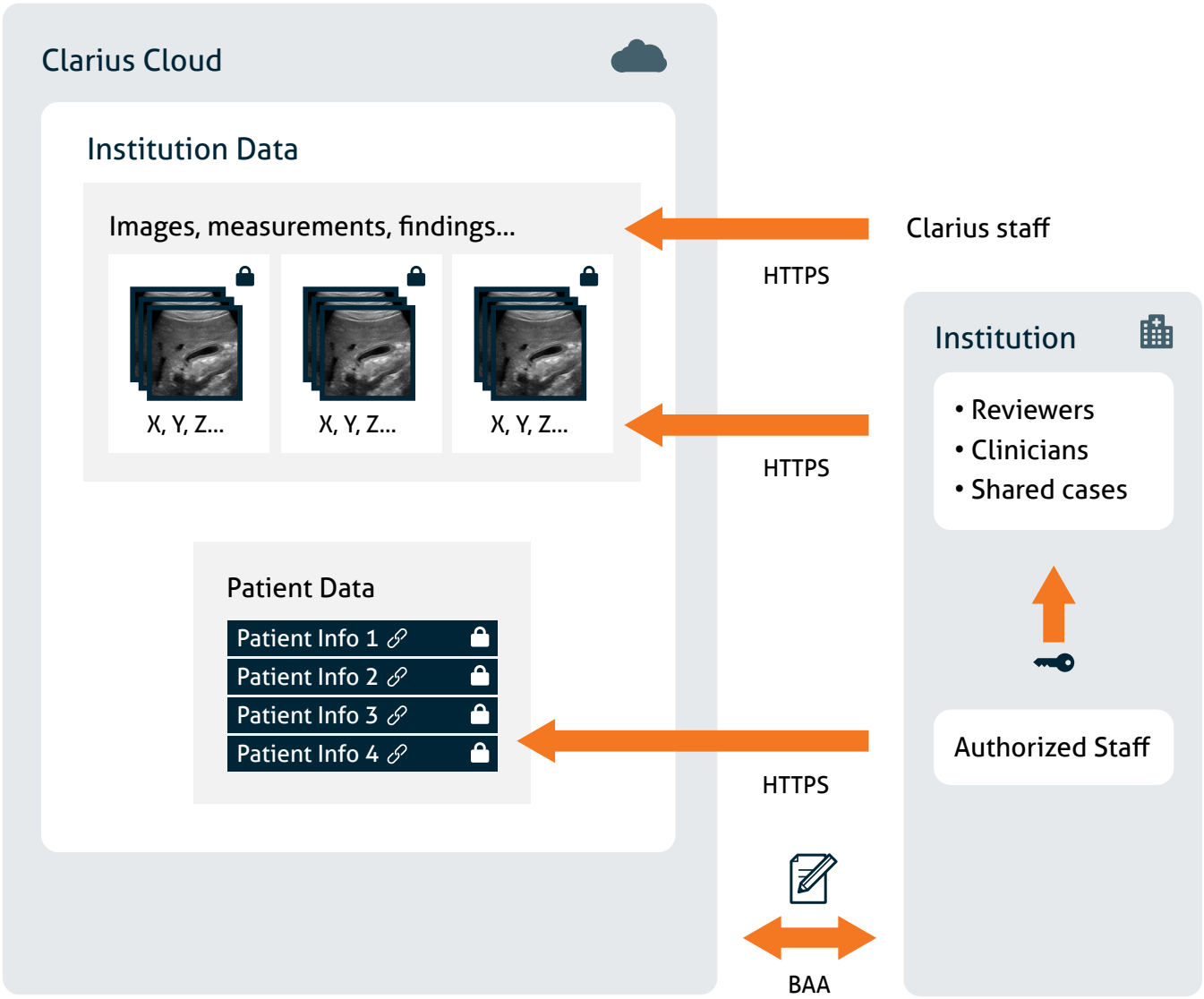
Camera Roll Export

Users have the option to export images to the device's local camera roll. This option is only available while data still resides within the separated App memory; once the retention timeframe has expired, local export will no longer be available. Exported images do not contain any PHI meta-data or burned-in PHI. In the future, a policy parameter will be available to completely disable camera roll export.

Clarius Cloud

Clarius Cloud is an online archiving tool developed fully in-house by Clarius for exclusive use by healthcare practitioners with a Clarius ultrasound scanner. By default, the Cloud is used for PHI permanent storage; however, users who want to store their exams on their own PACS are able to set up DICOM communications to bypass Cloud storage altogether. The Cloud is built on an Amazon Web Services (AWS) framework that allows for optimal security and scalability. Each Clarius Scanner comes pre-allocated with 2GB of secure storage on the Cloud. From a database perspective, PHI is stored separately from the actual ultrasound images, and both PHI and images are encrypted by default. Within an institute, only administrators and users who performed the examination can get access to the PHI and images stored.

Fig. 2
Clarius Cloud database access



Physical Storage & Data Residency Compliance

All data stored on the Clarius Cloud is stored in data centers located in Amazon Web Services' network. By default, data is stored in Canada. When users receive their first scanner, they are asked to setup a new institute on Clarius Cloud and specify the location of where PHI is to be stored. Clarius currently support the following regions:

- Canada (Montreal)
- United States (Oregon)
- EU (Frankfurt)
- Asia Pacific (Singapore)

Image data, patient records, business associate agreements, and audit logs are stored in the region specified by the user, while other institution data, such as exam metadata, institution members, and scanner information are solely stored in the main database located in Canada. There is no provisioning for migration of existing institutions from one region to another after the initial selection. Clarius does not store PHI outside of the Clarius Cloud.

Activity Logs

Operations involving PHI in the Clarius Cloud are logged and can be reviewed anytime by clients with administrative credentials. Logs cannot be changed and are stored for the six months, according to the retention policy. Logs can be exported for long term retention at the users' discretion.

Exporting Data

When reviewing an exam, the user has the option to export images. They are emailed a randomized link, which expires in 24 hours, to download a compressed file containing all the images within the exam, without any PHI included.

Accessibility and Credentials

Credentials are required to log into both the Clarius App and Clarius Cloud. On the Clarius App, the first login requires an Internet connection so that the credentials can be authenticated by the Clarius security infrastructure via Clarius Cloud. Afterward, users can continue to use the system for up to 90 days before re-validation of credentials is required. All passwords are encrypted using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by the National Institute of Standards and Technology (NIST). Clarius staff do not have access to view, change, or retrieve user passwords. If a user forgets or loses their password, the password can be reset through a temporary link emailed to the client, which expires after 24 hours. Clarius Cloud provides clients the ability to define password security policies, such as minimum length, complexity, expiration, and re-use parameters.

Compliance

HITRUST Security Framework

Clarius adopts the HITRUST Common Security Framework (CSF). The HITRUST CSF Assurance program is a common, standardized methodology to effectively and consistently measure compliance. The CSF tailors the requirements to a healthcare organization based on specific organizational, system, and regulatory risk factors, and integrates requirements from many authoritative sources, such as:

- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- GDPR (General Data Protection Regulation)
- And others

HIPAA

Clarius is compliant with HIPAA. As a business associate, Clarius follows the HIPAA Privacy Rule and the HIPAA Security Rule, in addition to the Breach Notification Rule. The HIPAA Compliance Statement can be found at **www.clarius.com/compliance**.

GDPR

Clarius complies with the General Data Protection Regulation (GDPR). PHI, images, and personal user data managed by Clarius, such as customer's personal and marketing information related to European persons, are covered under the compliance regime. The GDPR Compliance Statement can be found at **www.clarius.com/compliance**.

Retention

PHI and images on Clarius Cloud are stored for a minimum of seven years by Clarius. The Cloud system is backed up every hour, and the encrypted backups are stored and retained for 365 days.

Additional Operational Controls

Monitoring

The Clarius Cloud is continuously monitored (24 x 7 x 365) for security and operational purposes by Alert Logic. Traced events are stored in a Security Information and Event Management (SIEM) solution hosted by a third party. Actions that may threaten the environment or compromise the confidentiality of PHI are recorded and investigated.

Vulnerability Management

The Clarius Cloud regularly has comprehensive internal vulnerability checks with Tenable technology to validate the overall security of its system . The security of the Clarius Cloud is also validated by an independent third party.

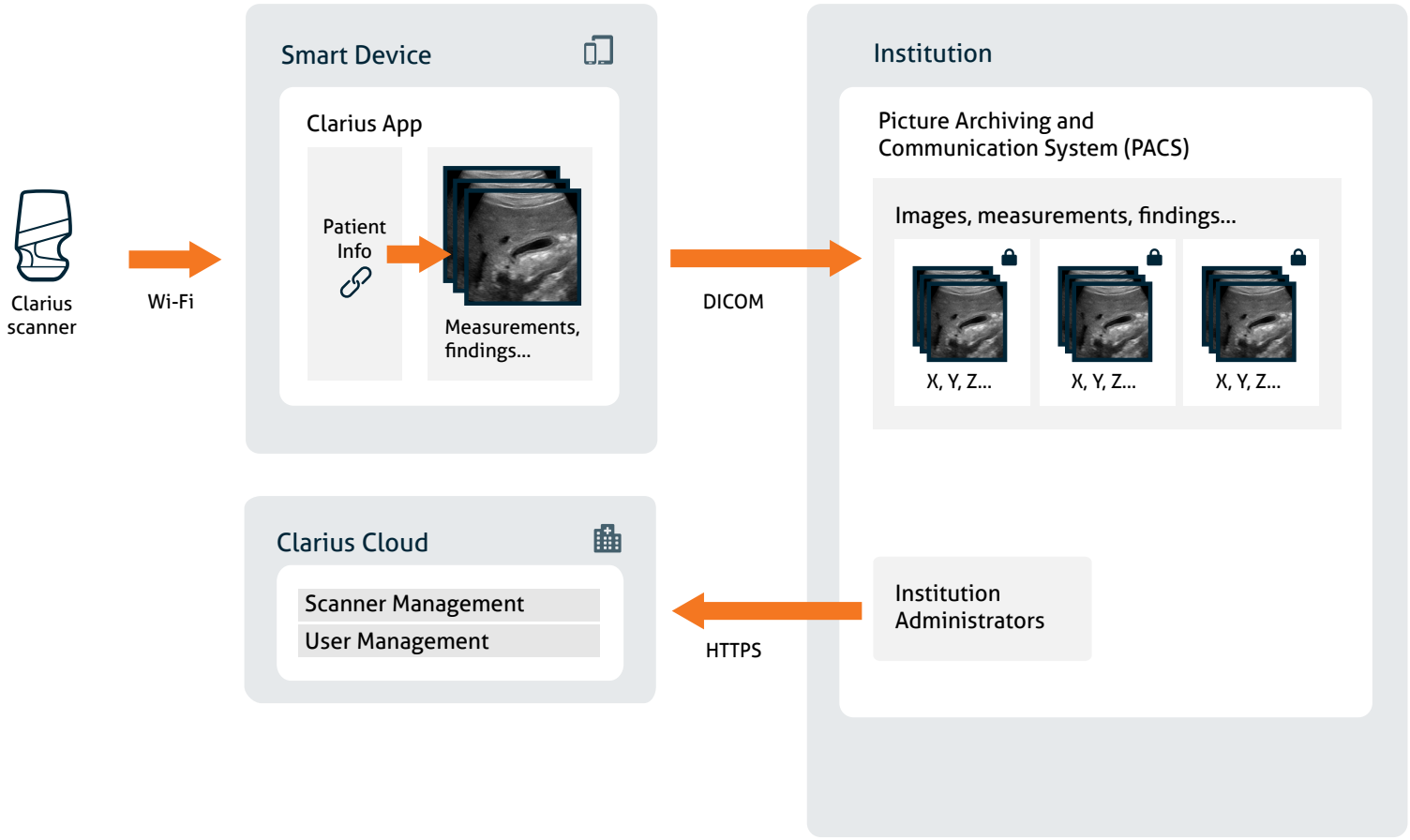
DICOM

The Clarius App can use DICOM Store to transmit PHI and examination data. DICOM network parameters are currently set up in Clarius Cloud by an administrator and transmitted to the App when the user initially logs in. Subsequent updates to information can be retrieved anytime the App has Internet connectivity on the mobile device. When storing data over DICOM to PACS, institutions can set a policy to prevent any data going to Clarius Cloud. Clarius does not provide encryption between the App and the customers' PACS. This security layer must be provided by the customer based on the network being used to transmit data.

Modality Worklist

Clarius also offers DICOM Modality Worklist support to retrieve PHI from a PACS supporting this function. When a user starts the App, they have the ability to choose a patient from a downloaded worklist. This worklist is only stored in physical memory while the App is running and is never stored to persistent storage.

Fig. 3
DICOM Store



Encryption Standards

The following summary lists the encryption types used between various modules within the Clarius ecosystem:

- Scanner to App Bluetooth: RSA256, AES128
- Scanner to App Wi-Fi: TLSv1.2 (control channel only)
- Scanner Wi-Fi Direct: WPA2
- App to Cloud: TLSv1.2
  - TLSv1.2 is FIPS 140-2 compliant and uses the following protocols: ECDHE-RSA-AES256-GCM-SHA384

Configurable Security Policies

Settings defined in the Clarius Cloud offer many policy configurations to help provide customers with the security tools required for their internal standards. These tools may apply to the Cloud, App, or both, and include:

- Password Security Requirements
- Two-factor Authentication (2FA) Requirements
- PHI Physical Storage Location
- Scanner Authorization
- Last Known Location
- Clarius Cloud Storage Permissions
- App Temporary Data Retention

The following features are currently in development:

- Scanner Credential Sync Timeframe
- App Logout Permissions
- PHI Mandatory Field Entry
- Camera Roll Permissions

Using Clarius Without the Cloud

Some customers may want to limit access to ePHI and Clarius Cloud if their institute security policies maintain a rigid structure and want to refrain from using any online tools. Clarius provides a solution that will allow its ultrasound devices to perform with a more traditional approach.

Fig. 4
Workflow to setup Clarius for use without Clarius Cloud

1. Create a single Administrator account on Clarius Cloud, managed by the IT department

2. Once logged into Clarius Cloud:

a) Set up appropriate DICOM information for storage and worklist servers → **b)** Set minimum scanner credential timeframe (eg. 365 days) **(Available upon request)** → **c)** Set password requirement to logout from Clarius App **(To be implemented)**

3. Log into Clarius App with Administrator account

4. Test Clarius Scanner and DICOM connectivity

5. Provide users with smart devices as required

Released May 29th, 2018