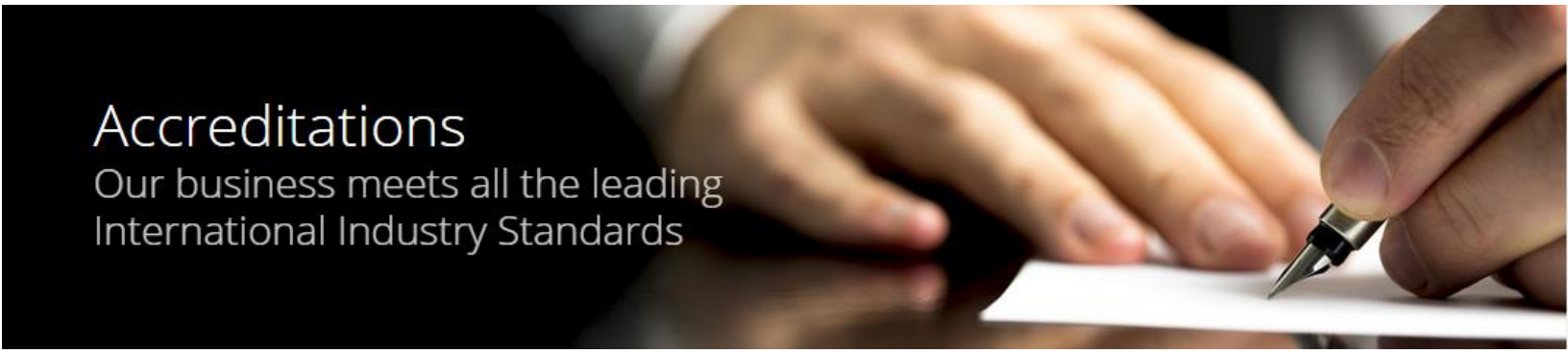

UK Cloud System Security and Compliance

Version: V5.2 - Dec 2019

Cimar and its technology partners (Ambra Health inc.), are committed to making privacy, security and integrity a priority in all Cimar products, services and implementations. This document addresses questions regarding the compliance, security practices and policies we employ in a straightforward, and transparent account of our systems, their hosting and their UK operation. We hope you find what you're looking for regarding security and compliance in this document. If there are any other questions regarding our policies and procedures, you may want to look at our Terms of Service and Privacy Policy available at https://cloud.cimar.co.uk or contact us for advice. Outside of this brief, questions can be directed to:

Howard Jenkinson
CTO – Cimar UK Ltd
h.jenkinson@cimar.co.uk

Security Summary

Cimar's Medical Imaging Management Platform service for sharing, storing and managing Medical Images (Radiology, Cardiology and other Medical Picture types) is in full compliance with relevant UK cloud service security requirements. The service:

- Is a hosted cloud service accessible only over HTTPS/TSL 1.2 encrypted connection.
- Is 2FA configurable per account, with enforced 'Strong' passwords and their periodic renewal.
- Can be embedded via REST API (JSON) into applications that will be sending or receiving clinical messages to or from your organisation.
- Can be integrated with SSO (Single Sign-on) systems (e.g. Active Directory)
- Is approved (Technically and DPIA) by numerous NHS Trusts and Private healthcare providers nationally.
- Every users access is role-based only, with constrained permissions by default.
- Meets UK Healthcare security standards for information Governance, GDPR, cloud-service 'best practice' for application methodology and architecture.
- Is hosted at UKcloud, a Crown Campus data centre co-hosting numerous HM Gov Public Services, Genomics England, and numerous NHS used apps)
- Is ISO27001 and ISO9001 accredited
- Is FDA 21CFR Part11 accredited
- Is G-Cloud 10 and 11 approved and listed
- All instances globally are HIPAA, IHE, DICOM, HL7 and Vendor-Neutral compliant.

The eTransfer solution and usage of the application platform at the heart of Cimar's cloud services are encrypted at all times – whether data is in transit or at rest.

System, data, communication, user, storage and platform security are explained in further detail below.

Our service is used extensively by UK healthcare organisations and is also embedded directly into health applications they use. Globally, the cloud platform hosts over 9bn images for 2,500+ hospitals and imaging orgs, 700+ Clinical Trials and over 5,000 clinics. Over 100,000 web-uploads occur per month currently serving a community of circa 1m clinical user logins per month.

UK Data Centre and SaaS Application Hosting

Cimar's cloud platform is hosted as an isolated secure environment at UK Data Centres: UK Cloud (https://ukcloudhealth.com). UKCloud is a leading UK Public Sector Data Centre host for numerous UK Govt Digital Public services. UK Cloud host UK sovereign, industry leading, multi-cloud platforms including Cimar's OpenStack cloud environment and many other healthcare applications. Cimar's hosting is secure, assured and located at the Government's Crown Campus. UKcloud Data Centres are Tier3 by design, set to DETER level security by default, and are located at Farnborough and Corsham.

Information Governance And Standards

The Data Protection Act (1998) and GDPR

This Act is the cornerstone requirement for all organisations that handle personally identifiable information. Cimar is a registered Data Processor with the Information Commissioners Office (ICO Ref ZA198618). The principles we follow for protecting patient data transacted through our systems and architecture, rigorously follow the pre-requisites of the DPA rules as applicable to the Data Processor and is in full compliance with GDPR requirements and law.

Data Sharing Agreements

Data being shared through Cimar's platform, is by agreement/arrangement between the sender and the receiver. Cimar is providing the means to share and plays no part in information that passes through the cloud, acting only as the Data Processor. Therefore, as is normal practice, it is the responsibility of data sharing parties/organisations to formalise permissions with patients and with those to whom such data is to be shared through the cloud. All activity relating to data passing through the cloud, who accesses it, when and with whom it is shares, is captured and recorded in extensive online audits for your account administrators to scrutinise and manage. Should you wish to establish a data sharing agreement with Cimar as well, we are happy to assist in the capacity of a Data Processor.

ISO 27001:20013

Cimar is an ISO27001:2013 Certified organisation (Ref QMS303492019). This standard is the UK's leading information security accreditation, with specific regard to information management, systems and framework to rigorously secure data undermanagement. Our corporate operational and hosting environments are ISO 27001 compliant ensuring all information we process and store is managed to the highest standards of information security. ISO 27001:20013 accreditation is important for any cloud-delivery service provider. Cimar is by design and from core platform level upwards, compliant and accredited accordingly.

ISO 9001:2015

Cimar's an ISO9000:2008 Certified organisation (Ref QMS14133334). Governed by the British Assessment Bureau, this standard is the UK's leading quality management accreditation and ensures the companies' operational technical procedures and workflows are well documented, effective and appropriate to ensure the optimal delivery of the service provided. Our entire software development, system architecture and release management is governed by ISO9001 accredited principles and framework. Our data centre also maintains this compliance independently.

FDA Approved - Indications for Use

FDA approval is generally regarded as the benchmark for qualifying appropriate diagnostic use of medical image viewers across the UK in accordance with CE approval. Information handling, storage and quality assurance also form part of this framework.

Cimar's platform originator is Ambra Health in the US. Our zero-footprint DICOM functionality is FDA approved as a class 1 medical device.

FDA number is 3008776294.
510(k) Number: K152977
Device Name: DG PACS
Prescription Use (Part 21 CFR 801 Subpart D).

Cimar Cloud-PACS software is intended for use as a primary diagnostic and analysis tool for diagnostic images for hospitals, imaging centres, radiologists, reading practices and any user who requires and is granted access to patient image, demographic and report information. Cimar's Viewer, a component of our Cloud PACS, displays and manages diagnostic quality DICOM images. Cimar's Viewer is not intended for diagnostic use on

mobile devices and alerts the user accordingly. If used on conventionally suitable diagnostic equipment, the viewer is qualified as a diagnostic viewer.

HIPAA

Cimar's Cloud-PACS platform is HIPAA compliant by design, and employs patented security technology that keeps patient information safe and compliant to HIPAA standards at all times. Image data is shared (manually or automatically) via a secure encrypted web connection and can only be accessed by authorised personnel. Patented split-merge technology anonymises study images by removing protected health information (PHI) from imaging data. The PHI is separately encrypted and stored, creating an Internet-safe study image – it is un-identifiable when in transit or at rest. In addition, all data transacted between source is exchanged over secure HTTPS/SSL, losslessly compressed 256bit encrypted connections, meeting UK Govt e-GIF standards for the digital exchange of patient identifiable information.

G-Cloud 11

Cimar is a G-Cloud 11 qualified supplier (Service ID 848175195806931 + 5 others) and listed as an accredited service provider on HM Gov's G-Cloud platform (Crown Commercial Service). This enables public services to procure from pre-vetted and approved cloud service providers, that meet the compliance requirements expected by public service organisations.

Assured Secure Communications

In transit, all our eTransfer solutions use AES256 bit SSL encryption over HTTPS /TLS 1.2 and automatically applied lossless compression. Whether in transit or archive, imaging data are stored separately from all Patient Identifiable information (PHI Meta-Data). Uniquely, (See Split-Merge technology guide), imaging data is automatically split apart from DICOM PHI in memory, and encrypted so that images are never stored on the same servers as corresponding encrypted PHI data.

All user logins use and viewing of information on, to or from our systems, is also over HTTPS with encryption. The only port over which we communicate meta and data information (encrypted) is 443.

There are two primary eTransfer methodologies for routing imaging and reports to the cloud. Both are over HTTPS, and both support auto-anonymisation if required.
Manual Web-Upload: from any browser, anywhere, a user can upload DICOM CD/DVD or folder content fast and seamlessly. This functionality can be embedded within other applications via Cimar's REST API.
Automated and Direct Routing: by installing a low-footprint cloud gateway utility, images (DICOM) and reports (HL7) can be sent directly from source systems via set AET connectivity. Any PC or server can host the gateway install, which requires network config to communicate to DICOM node inside a client network. All communications from the gateway are outbound only. Details of Cimar's gateway technology can be found in our Technical manual which can be supplied as required. For clients that implement fully automated DICOM Gateway functionality within their networks, communications to the cloud are still only over encrypted HTTPS/SSL connections (port 443).

If your firewalls or proxy scripts block such access, then you may need to add permission rules to allow your users access to https://cloud.cimar.co.uk (IP address 51.179.219.63).

Web Application Access Security

Our service is provided as a secure platform for sharing and reporting on images. This security is at many levels. Your administrator has considerable control of system settings, and default configurations and of all your users. Your administrator is responsible for the configuration and correct settings to ensure information workflows operate as per your Organisation's needs, and within the prevailing UK laws and standards for sharing patient information.

Every end user must have a unique username and password which allows them access to their Worklist account only. The FDA accredited system and its web-viewer include detailed audit trails of every event and user action and DETER level rigorous monitoring and testing is conducted to ensure the security of this cloud based system is assured.

Web access Passwords and user authentication

All users of the system are invited or created by your administrator who generates a user account login for them. Once acknowledged by the user, their password is prompted for

change.

- 2FA authentication can be configured in accounts if required.
- In addition, your Administrator can set the system defaults to force all users to change their passwords every 30, 60 or 90 days.
- Password strength is enforced, requiring a combination of Alpha Numeric characters, with a minimum acceptable length of 10 elements. No passwords can be re-used.
- Your administrator is able to suspend, change, delete and modify user access permissions (Role-based) as required by you as the account controller, at any time.

User access of an account can be constrained to permit access only from specific IP addresses. A "whitelist" of IPs (or ranges) can be configured per account in the cloud.

Permitted user - Role-Based functionality

Cimar's cloud application provides a Role Based console to create customised permission templates, each for differing types of users and the functionality they are permitted – or actively denied.

For example administrators are able to manage an account at granular level, but a patient or consultant should only be able to login to their worklist, and only see or add to their data – that's it. A vast range of options in between these extremes can be configured by client administrators.

When a user is added to the system, they are allocated a default role at the lowest functional level – this template entitles them to limited functions you permit or deny. There are over 200 variable permissions and 1000's of functionality combinations that can be set for user roles. This enables you to ensure rigid, precise and specific access to both your system records and permissible functionality.

Technical Configuration

Acceptable Encryption Policy

All Cimar encryption utilises NIST approved cryptographic modules. Common and recommended ciphers include AES 256, Triple DES and RSA. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys are of a length that yields equivalent strength. Cimar's cloud-PACS Service key length requirements are reviewed annually as part of the yearly security review and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose. The service conforms to and exceeds UK eGIF regulations, a Cabinet directive defining the encryption type and standards used when patient or other data belonging to a UK citizen are transmitted electronically.

Ownership and Responsibilities

All internal servers deployed for the Cimar Cloud-PACS host platform are owned and operated by Cimar UK. Cimar is responsible for overall system administration. We monitor configuration compliance and implement an exception policy tailored to our Data Centre providers' hosted environment.

- Servers are registered within the Hosts corporate enterprise management system.
- Main functions/applications, and applicable Information in the corporate enterprise management system, is proactively kept up to date.
- Configuration changes for production servers follow our approved and appropriate change management procedures.

Monitoring

All security related events on critical or sensitive systems are logged, and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 year.
- Weekly full backups of logs will be retained for at least 1 year.
- Monthly full backups will be retained for a minimum of 2 years.

Security related events are reported to Operations, who will review logs and report incidents to Operations management. Corrective measures will be prescribed as needed. Security related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorised or abused access to accounts
- Anomalous occurrences that are not related to specific applications on the host.

Related Conformance Documents

Compliance Statements

- Cimar - DICOM Conformance Statement.pdf
- Cimar - HL7 Guide.pdf
- Cimar-UKC-GEN-629 GDPR Evidence Pack v.1.0.pdf (under NDA)
- Cimar-UKC-GEN-SEC0012v10.1 (Updated for G-Cloud 11).pdf (under NDA)

Technical Resources

- Cimar - Gateway Guide (Cloud).pdf
- Cimar - RESTful Public API V3 Guide
- Cimar - Split-Merge Encryption and Transmission Technology.pdf