RealAppleIQ™ Suite

Client Data Protection Overview

What happens to your data, how it is protected, and who can see it

Document Reference:	RIL-RAQ-CDP-001
Version:	1.0 02-06-2026
Issued By:	Real Instruments Limited
Audience:	Clients, IT departments, and legal teams
Purpose:	Plain English and technical explanation of data protection measures

A Plain English Explanation

We know that handing your measurement data to any system raises a question: could someone else see it? This section answers that question honestly, without technical jargon. If you want the full technical and legal detail, it starts at Section 1.

Your data is locked to your licence

When the RealAppleIQ™ instrument finishes a measurement run, the data it produces is immediately assembled and locked using your unique licence credentials. Five pieces of identifying information are built into every data file: your licence details, the software type, your operator name, the device name, and the serial number of the instrument. These identifiers are not just labels — they are part of the lock. Without the right combination, the file cannot be opened.

The data file is then encrypted before it is stored or uploaded. The encryption uses a current industry-standard algorithm. Even if someone were to obtain the raw file, they would have an encrypted package that is meaningless without both the decryption key and a deep understanding of Real Instruments' proprietary internal data format.

> Think of it this way: even if someone could break the lock on the front door, everything inside is written in a language only we understand. The data has no value to anyone outside Real Instruments and the client it belongs to.

Video files are handled differently

Video recorded during a measurement run is not encrypted. It is stored on the primary pc device in its native format. Video data uploaded is stored on the server fragmented in blobs. These are secured by five identifying licencing credentials.

We recommend that clients who have concerns about video content consider conducting measurement runs without video recording. The measurement data itself is fully encrypted and is not affected by this choice.

Only your software can see your files

RealDataIQ™ — the viewer application used by your team — will only display files that match all five of your identifying credentials. If any one of those credentials does not match, RealDataIQ™ either will not open at all, or will show no files. This applies to files on the server, files on a local device, and any files that have been copied from another device. There is no way to open one client's files on a different client's system.

Your licence key is your responsibility

The licence key issued to your organisation is, in effect, the master key to your data. Real Instruments Limited issues it to your primary contact. What happens to it after

that is your organisation's responsibility. We strongly recommend treating it with the same care as any other critical access credential.

The same applies to any sub-licences you issue to third parties. When you issue a sub-licence, you control exactly which runs are shared and for how long. But once issued, the responsibility for that access rests with you.

Who at Real Instruments can see your data?

Access to client data within Real Instruments Limited is restricted to one person: our Chief Technology Officer. This access exists solely for the purposes of technical support and system maintenance. No other Real Instruments staff can access your data.

⚠ Important: Real Instruments Limited holds a copy of your data on its servers to enable access by your team. This is not a backup service. You are responsible for maintaining your own backup of all data and video on the primary laptop.

1. Data Collection and Encryption

This section describes how data is created, identified, and secured at the point of collection.

1.1 Measurement and Data Assembly

A measurement session is initiated using the RealUserIQ™ software on the primary laptop, with the RealAppleIQ™ instrument connected. At the conclusion of a run, RealUserIQ™ assembles the raw measurement data using a proprietary mechanism into a binary file (binfile). This assembly process is not a standard or published format.

1.2 Identifying Credentials

Five identifying credentials are embedded into every binfile at the point of creation:

Credential	Description	Purpose
Licence file information	The client's unique licence details	Ties the file to a specific client account
Application type	Identifies the RealAppleIQ™ software variant	Prevents cross-application access
Operator name	The RealUserIQ™ user account	Ties the file to a specific operator
Device name	The name of the primary laptop	Ties the file to a specific device
Instrument serial number	The unique serial number of the RealAppleIQ™ instrument	Ties the file to a specific physical instrument

1.3 Encryption of Binfiles

Following assembly, each binfile is encrypted using a current industry-standard encryption algorithm. RSA-2048-OAEP / AES-256-CBC Hybrid Encryption key protected and signed.

The encryption key is managed separately from the licence credentials and is not stored on the client's device. Encrypted binfiles are stored on the primary laptop and uploaded to the Real Instruments Limited database by RealBaseIQ™.

> Note: Even in the unlikely event that an encrypted binfile were obtained and decrypted, the resulting data would be in Real Instruments' proprietary internal format. Interpreting this data requires detailed knowledge of that format, which is not publicly available.

1.4 Video Files

Video files recorded during measurement sessions are not encrypted at the file level, either on the primary laptop or on the Real Instruments Limited server. Instead, video is stored as a collection of binary fragments in the database. Stored fragments cannot easily be assembled into a viewable file.

Recommendation: Clients with concerns about video confidentiality are advised to conduct measurement runs without video recording. This eliminates video data from the system entirely. Measurement data (binfiles) is not affected by this choice and remains fully encrypted.

2. Data Storage and Hosting

Item	Detail
Primary storage location	Primary laptop (supplied by Real Instruments Limited)
Cloud storage provider	Real Instruments Limited. While final security protocols are tested and confirmed. Transition to a large, recognised provider such as sitehost.nz will begin soon.
Server location	New Zealand
Data format on server	Encrypted binfiles; video stored as credential-locked blob fragments
Data retention on termination	Archived. Data is retained in an archived state following contract termination and is not actively deleted.
Backup responsibility	Client. Real Instruments Limited's server copy is not a backup service and is not guaranteed as one.

3. Access Controls

3.1 Licence-Based Access

Access to all data in the RealAppleIQ™ system is governed by the five identifying credentials described in Section 1.2. RealDataIQ™ validates all five credentials on launch and when accessing any file. A mismatch in any credential results in one of the following:

Outcome	Condition
Application does not open	One or more credentials are invalid or absent
No files visible	Application opens but no files match the credential combination
File not accessible	A specific file's embedded credentials do not match the active licence

This behaviour applies equally to files on the server, files on a local device, and any files that have been copied from another device — whether within the same organisation or from an external source.

3.2 Primary PC Restriction

The RealUserIQ™ measurement software can only operate on the designated primary laptop. The primary laptop is the only device on which measurement

sessions can be conducted. Changing the primary laptop requires contacting Real Instruments Limited to enable a primary PC change. Physical connection of the RealAppleIQ™ instrument to the new pc and acceptance of transfer conditions will enable moving of primary identifier.

3.3 Real Instruments Limited Staff Access

Role	Access Level
Chief Technology Officer	Limited access to client data for technical support and system maintenance purposes only
All other Real Instruments staff	No access to client data

4. Sub-Licence Access

4.1 Sub-Licence Architecture

Sub-licences allow the primary account holder to grant a third party access to a defined selection of measurement runs. The following security controls apply to all sub-licences:

Control	Description	Controlled by
Run selection	The primary user specifies exactly which runs the sub-licence holder can access. The sub-licence holder has no visibility of other runs.	Primary account holder
Duration	The sub-licence has a defined expiry date set by the primary user.	Primary account holder
Download limit	The maximum number of downloads permitted under the sub-licence is set by the primary user.	Primary account holder
Credential matching	Sub-licence holders must present a matching identifier — set by the primary user at the time the run is selected for sharing — to access any file.	Real Instruments Limited (technical enforcement)
Distribution	The sub-licence package (including software installer) is sent to the primary client's nominated contact for onward distribution. Real Instruments Limited does not distribute sub-licences directly to third parties.	Primary account holder

4.2 Sub-Licence Encryption

The sub-licence file itself is encrypted and contains the access parameters described above. The terms of the sub-licence (duration, download limit, run selection) cannot be modified by the sub-licence holder.

4.3 Video Under Sub-Licence

Video shared with a sub-licence holder is not encrypted at the file level. Clients who do not wish sub-licence holders to view video associated with a run are advised to conduct that run without video recording.

⚠ Responsibility for sub-licence use rests with the primary account holder. Real Instruments Limited issues the sub-licence to the client's nominated contact. The client is responsible for its distribution and for any access that results from it.

5. Data Transmission

All data transmitted between the primary laptop and the Real Instruments Limited database is encrypted prior to transit. Transmission is handled by RealBaseIQ™, which operates automatically in the background. Clients do not need to initiate or manage upload processes.

Transmission type	Security
Binfile upload (primary laptop → server)	Encrypted on creation; file is already encrypted before upload
Video upload (primary laptop → server)	Transmitted securely; stored as blob fragments on server
Analyst download (server → Analyst device)	Encrypted prior to transit; credential validation required before download initiates
Sub-licence download (server → third party)	Encrypted prior to transit; sub-licence credential validation required
Software updates and licence delivery	Encrypted prior to transit. RealBaseIQ™ manages files upon authentication.

6. Client Responsibilities

Real Instruments Limited is responsible for the security controls described in this document. The following responsibilities rest with the client:

Responsibility	Detail
Licence key security	The licence key issued to the client is the master credential for all client data. The client is responsible for controlling who holds it and how it is used.
Sub-licence distribution	Sub-licences are issued to the client's nominated contact. The client is responsible for all onward distribution and for any access that results.
Data backup	Real Instruments Limited holds a server copy of client data to enable access. This is not a backup. The client must maintain an independent backup of all data and video on the primary laptop.
Primary laptop security	The primary laptop is the only device capable of conducting measurement sessions. The client is responsible for the physical security and access control of this device.

Video recording decisions	Where video confidentiality is a concern, the client should consider conducting runs without video recording. This is a client decision and is not managed by Real Instruments Limited.

7. Summary: Security at Each Stage

Stage	Security measure	Notes
Data assembly	Proprietary binary format; 5 embedded credentials	Non-standard format with no public specification
Binfile encryption	Industry-standard encryption AES-256 encrypted, RSA-2048 key protected and signed	Key managed separately; file unreadable without key + format knowledge
Video storage	Not encrypted on primary pc. Blob fragment architecture on database. Credential-locked reassembly	Fragments are not viewable individually
Data transmission	Encrypted prior to transit	All upload and download traffic
Server storage	Encrypted binfiles; blob video fragments; credential-gated access	Real Instruments Limited. While final security protocols are tested and confirmed. Transition to a large, recognised provider such as sitehost.nz will begin soon.
Access control	5-credential matching; licence-based gating	Mismatch → no access; applies to all devices and file copies
Sub-licence access	Encrypted sub-licence file; credential matching; client-controlled run selection and limits	Client responsible for distribution
Real Instruments staff access	CTO only; limited to support and maintenance	No other staff access