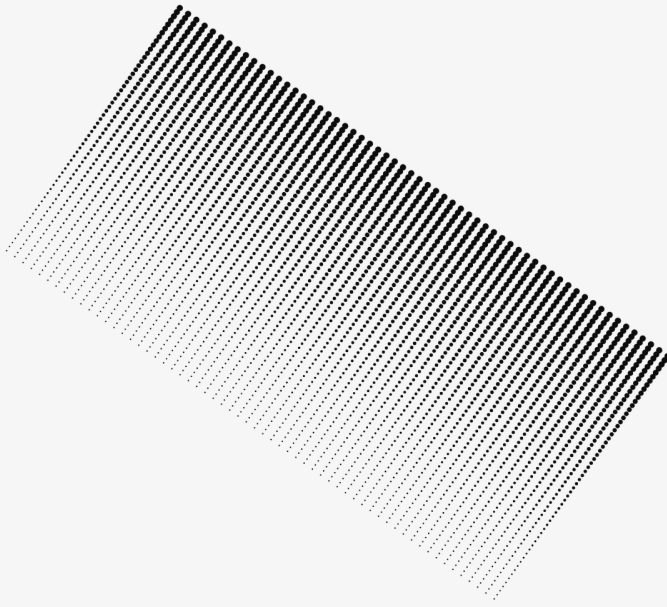




GUIDE 07 DEVICE DATA

What the device recorded

Event logs, alarm logs, trends, and settings: where a device keeps its own record of the event, how to get it out intact, and how to read it.



ABOUT

Most devices made in the last twenty years keep a record of what they did. The record is written by the device, at the time, without anyone deciding what to say. It is often the only witness that was present for the whole event.

This guide explains what a device records, where the data is kept and how long it survives, how to get it out without changing it, and how to read a log against the clinical record and the clock. It is written for people who will not do the download themselves but must decide who does, and must judge what comes back.

FOR

Legal counsel who must establish the sequence of events from the device's own data, and protect that data from the first day.

Manufacturers — complaint, service, and engineering teams who download and interpret logs.

Hospitals — clinical engineering and risk management staff who hold the device after an event.

NOTE

This guide is general technical information. It is not legal advice. Log formats, retention, and the tools needed to read them differ by device and by software version; the manufacturer's service documentation is the authority for each.

In this guide

01	What a device records	04
	Figure: where the data lives, and how long	05
02	Before the download	06
03	The download	08
04	Reading the log	09
05	What a log can and cannot say	10
06	Where the record is weak	11
	Checklist	12
	Sources	13
	How Alpha Devices helps	14
	Terms	15

01 What a device records

A device records what its software was written to record. The categories below are common to infusion pumps, ventilators, monitors, anaesthesia machines, dialysis systems, and most other equipment with a processor. Not every device keeps all of them, and the names differ.

EVENTS	Power on and off, mode changes, start and stop of therapy, user actions at the keys, doors opened, sensors connected, self-test results. Each entry has a time stamp and a code.
ALARMS	Each alarm condition with its priority, the time it began, the time it ended, and often what the user did: silenced, paused, acknowledged, changed a limit. Some devices also record what the alarm sounded as.
TRENDS	Measured values sampled at an interval: pressure, flow, rate, volume, temperature, battery. The interval sets what the trend can show. A value sampled once a minute cannot show a four-second event.
SETTINGS	The configuration in force, and the history of changes: limits, drug library version, ventilation mode, default profiles. Some devices keep an audit trail of who changed what; many keep only the current state.
FAULTS	Error codes, software exceptions, hardware self-test failures, communication time-outs. Often in a separate technical log reachable only with a service tool.
SERVICE	Hours run, cycles, calibration dates, parts replaced, software versions installed and when. The device's own service history, independent of the paper file.

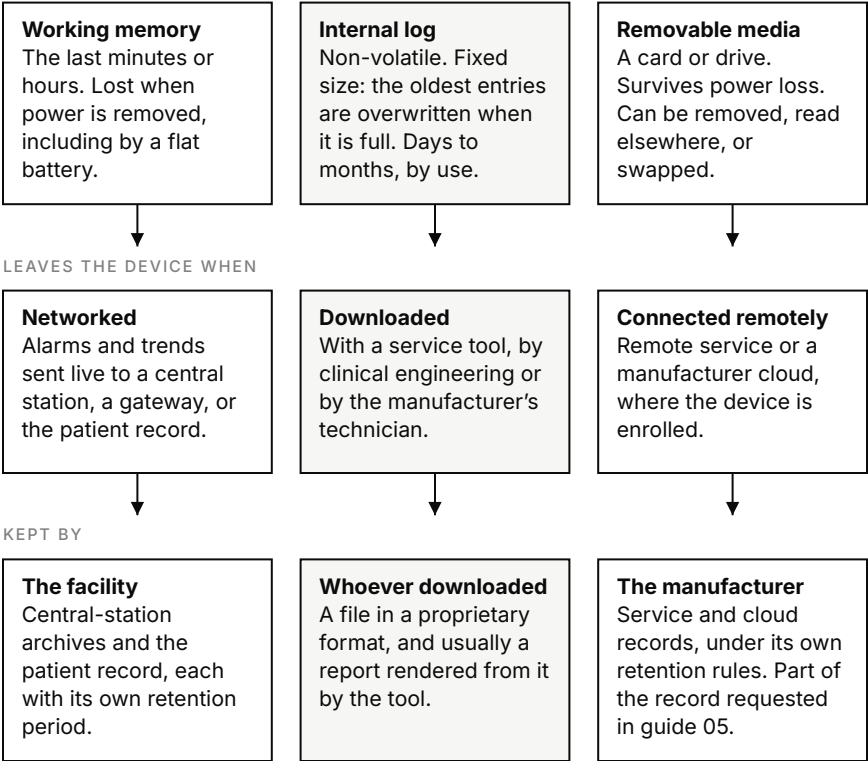
NOTE

Ask the manufacturer for the log specification: the list of every code the device can write, what each means, and what triggers it. It is a design document (guide 05) and it decides what the log can prove.

FIGURE

Where the data lives, and how long

IN THE DEVICE



Each box is a separate copy with its own retention. The internal log is the one that overwrites itself; it is the first to secure, and the most likely to be gone.

FIG 01

The same event may exist in four places and in none. Working memory goes at power off, the internal log wraps, the download depends on the tool, and the network copy depends on what the device was set to send.

02

Before the download

A log is changed by the ordinary handling of the device. These rules keep it as it was at the moment of the event; they belong with the preservation steps in guide 01. Until a download procedure is agreed (section 03), nobody downloads.

01

Leave the power state as it is

If the device is off, do not turn it on: start-up writes entries and may run a self-test. If it is on, do not turn it off: working memory and some trends go with the power. Keep it on mains and note the battery state.

02

Do not clear, reset, or service

No "clear alarms", no reset, no software update, no maintenance, no calibration. A service visit between the event and the download is the most common way a log is lost.

03

Photograph the screen and the clock

The displayed time next to a phone showing real time, with the date. The offset between device time and real time is the first thing needed to read the log, and the hardest to recover later.

04

Record the configuration

Software version, serial number, accessories, media, network connections. Photograph labels and the version screen if it is already shown; do not navigate menus to find it.

05

Secure the removable media in place

Leave a card or drive in the device. Removing it, or reading it in a computer, can change the file system and the time stamps.

06

Hold the network copy

Ask the facility to preserve the central-station archive and the patient-record interface data for the period, before their own retention clears them.

NOTE

These rules apply to every copy of the data: the device, the removable media, the central station, and the manufacturer's remote connection. A copy that has been changed is a copy that has to be explained.

03 The download

Most logs can be read only with the manufacturer's service tool, and the tool is usually in the manufacturer's hands. That is not a reason to let the download happen without a protocol. It is the reason to write one.

01 **Agree the procedure first**

Who runs the tool, who watches, what is connected, which functions of the tool will be used and which will not. Service tools can clear logs, reset counters, and update software as easily as they read. The protocol names the read-only functions and excludes the rest. Guide 08 covers the joint protocol in full.

02 **Take the raw file, not only the report**

The tool produces a file in the manufacturer's format, and often a report rendered from it: a PDF or a spreadsheet. The report is an interpretation; it applies filters, rounds values, and omits codes the tool's author thought were not of interest. Ask for the raw file, the tool's version, and the specification that decodes the file.

03 **Fix the copies at the moment they are made**

A hash of each file, computed when it is written and recorded in the protocol, establishes that the file read later is the file that was taken. Copies go to each party at the same time.

- **CAUTION**

- A download by the manufacturer alone, with the device then returned to service or sent for repair, leaves one party holding
- the only copy of the only witness. Guide 01 explains why the
- device should not be returned at all until the record is complete.

04 Reading the log

A log is a list of coded entries with time stamps. Reading it is translation, alignment, and comparison, in that order.

01 Establish the clock

Device time against real time, from the photograph taken at preservation. Check for time-zone and daylight-saving settings, a clock reset at power-up, and drift over a long deployment. Every later comparison depends on this offset.

02 Translate the codes

Each code against the log specification or the service manual. Keep the code next to the translation; a translation alone cannot be checked.

03 Build the sequence

Events, alarms, faults, and setting changes on one list in device time, with real time alongside. Trend values are added where they change the picture.

04 Align with the clinical record

Nursing notes, the medication record, the monitor archive, and the patient-record interface, each with its own clock. Where the records disagree on time, say so; do not pick one silently.

05 Look for what is missing

Gaps in the sequence, a log that begins after the event, entries overwritten by a wrap, a self-test at a time nobody reports touching the device. Each gap is a finding, and the preservation record should explain it.

06 Compare settings before and after

The configuration during the event against the default profile and against the configuration when the device was downloaded. A change in between was made by someone.

05

What a log can and cannot say

A log is written by the device about itself. It says what the software detected and chose to record, at the resolution the designer chose. That is a great deal, and it has edges.

IT CAN SAY

What mode the device was in, what it measured, which alarms it raised and when, what keys were pressed, what faults it detected, and what version of software was doing all of this.

IT CANNOT SAY

Whether an alarm was heard, what was happening to the patient between samples, what a sensor that was not connected would have measured, or why a user pressed a key. Those come from other records and from testing.

ABSENCE

An event that is not in the log either did not happen, or happened and was not logged, or was logged and overwritten. The log specification separates the first from the second; the preservation record separates the second from the third.

LOGGING IS A FUNCTION

The design file contains requirements for what the device logs, and verification that it does. Where the log is central, ask for those (guide 05). A logging function that was never verified is a log that may not say what it seems to.

KEY POINT

Read the log as the device's own statement: precise about what it was designed to notice, silent about everything else. The log specification draws the line between the two.

06

Where the record is weak

These are the findings an engineering reviewer looks for first when a log arrives. Each one changes what the log can be used for.

01

No clock reference

Nobody recorded device time against real time. The sequence stands; its alignment with the clinical record does not.

02

A service visit in between

Maintenance, calibration, an update, or a repair between the event and the download. Ask for the service record and the tool log of that visit.

03

A report without the file

A rendered PDF with no raw data, tool version, or specification. It cannot be checked against anything.

04

A wrapped log

The oldest entry is later than the event. The log's size and the rate of entries say how long it holds; the preservation record says why the download was late.

05

Versions that do not match

The version in the log, on the label, and in the facility's inventory differ. Each is a question about what was installed when.

06

Settings with no history

The device records the current configuration, not changes. Who set a limit, and when, has to come from the facility's records or from testimony.

NOTE

A weak log is still evidence. The point is to state what it establishes and what it does not, before someone else does.

CHECKLIST

Device data at a glance

- ☐ Power state left as found; device on mains; battery state noted
- ☐ No clear, reset, update, calibration, or service since the event
- ☐ Screen and clock photographed against real time, with date
- ☐ Serial number, software version, accessories, and media recorded
- ☐ Removable media left in place
- ☐ Central-station archive and patient-record interface data preserved by the facility
- ☐ Download protocol agreed: who, which tool, which functions, who watches
- ☐ Raw file, rendered report, tool version, and log specification obtained
- ☐ Hashes recorded at download; copies to each party
- ☐ Clock offset established; codes translated with the code kept alongside
- ☐ Sequence built in device time and real time; aligned with the clinical record
- ☐ Gaps, wraps, version mismatches, and setting changes listed as findings

SOURCES

Sources and further reading

eCFR — 21 CFR Part 820, Quality Management System Regulation (820.35, complaint and servicing records)

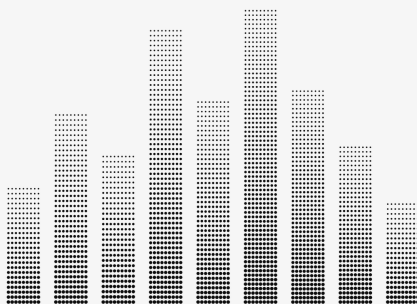
[ecfr.gov](https://www.ecfr.gov)

IEC 60601-1-8 — Medical electrical equipment: general requirements, tests and guidance for alarm systems (with amendments 1 and 2; alarm system logging provisions)

[iec.ch](https://www.iec.ch)

Alpha Devices — Guide 01, A device failed. What happens next?; Guide 08, The joint inspection

[alphadevices.io](https://www.alphadevices.io)



SERVICES

We get the data out intact, and read it as engineers

We write the download protocol, attend the download, decode the raw file against the manufacturer's specification, and build the sequence with the clinical record and the clock.

01

Preservation and protocol

Instructions for the first day, and a download protocol that names the tool, the functions, and the witnesses.

02

Decoding and sequence

The raw log translated code by code, aligned to real time, and set against the clinical record on one timeline.

03

Testing what the log implies

Where the log shows a fault or an alarm pattern, we reproduce the conditions on an exemplar device and record what it logs.

TERMS

Terms used in this guide

Event log

The device's list of what it did: power, mode changes, user actions, self-tests, each with a time stamp and a code.

Alarm log

Each alarm condition with its priority, start and end time, and what the user did about it.

Trend

Measured values stored at a fixed interval. The interval sets what the trend can show.

Non-volatile memory

Storage that keeps its contents without power. Usually of fixed size, overwritten from the oldest entry when full.

Service tool

The manufacturer's software or hardware for reading a device's internal data and for servicing it. Many can also write.

Log specification

The design document that lists every code the device can write, what it means, and what triggers it.

Clock offset

The difference between the device's clock and real time, measured by photographing the two together.

Hash

A short fixed value computed from a file, which changes if the file changes. Recorded at download to prove the file is unchanged.

Tell us about the device.

Send a short description of the device, the event, and any deadlines. We will tell you what to preserve now and recommend the next steps.

EMAIL info@alphadevices.io

WEB alphadevices.io

GUIDES

- | | | | |
|----|-------------------------------------|----|--------------------------------------|
| 01 | A device failed. What happens next? | 09 | How a device reaches the market |
| 02 | Searching MAUDE with purpose | 10 | Why the alarm did not help |
| 03 | Understanding waterfall design | 11 | When the software is the suspect |
| 04 | Reading an ISO 14971 risk analysis | 12 | Use error is a design question |
| 05 | The manufacturer's record | 13 | Complaints, MDRs and CAPA |
| 06 | Using LLMs to review case documents | 14 | Recalls, corrections and quiet fixes |
| 07 | What the device recorded | 15 | What did they know, and when? |
| 08 | The joint inspection | | |

Alpha Devices

2101 Brandywine Street, Suite 200
Philadelphia, PA 19130

Independent medical device engineering. © 2026 Alpha Devices.

