



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Wearables and Fitness-Tracker Forensics

Heart Rate, Steps, Sleep and GPS: The Body's Digital Diary

A smartwatch or fitness tracker is worn against the body all day and most of the night, and it records what the body does: heart rate second by second, steps and movement, sleep and waking, and, on GPS-equipped devices, exactly where a run or walk went. Most of this is not really stored on the watch, which is a small relay, but synced through a phone app to the manufacturer's cloud, where the detailed history lives. For a lawyer, this makes the wearable a witness of a peculiar and intimate kind: it can show that a person was active, moving or at rest at a precise time, place them on a route, and sometimes reveal that a claimed injury, alibi or timeline does not fit the body's own record. It can also, on rare and serious occasions, mark the moment a heart stopped. But wearable data is intimate health data, its accuracy varies, and it records the device, not certainly the person, so it must be obtained lawfully, corroborated and honestly bounded. This guide sets out for UK lawyers what wearables record, where that data lives, how it is preserved and extracted, and how it is deployed with care.

© Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Wearable-device work spans the watch, the paired phone and the manufacturer's cloud: extraction of on-device data, recovery of the app's synced records, and lawful collection of the detailed cloud history of activity, location and health metrics: correlated with other sources, handled with the heightened care that health data demands, and reported under CPR Part 35 and CrimPR Part 19 with the accuracy and limits of the data stated plainly.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

WEARABLE & APP EXTRACTION

CLOUD HEALTH-DATA COLLECTION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: the body keeps a log
03	What wearables record, and where the data lives
04	The watch, the phone and the cloud: the sync chain
05	Preserving and extracting wearable data
06	Accuracy, attribution and honest limits
07	Deployment: timelines, injury, location and health-data sensitivity
08	Source architecture: where else the evidence lives
09	Worked examples
10	Common mistakes and technical limitations
11	Questions to ask · Suggested wording
12	Checklist and red flags · When to involve a digital forensic expert
13	Frequently asked questions
14	Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

The headline point: a wearable records the body's activity, heart rate, steps, sleep and often GPS, but keeps little on the watch itself: the detailed history lives in the phone app and the manufacturer's cloud, so the evidence is reached through the account, obtained lawfully, corroborated, and bounded by its accuracy and by the fact that it records the device, not certainly the wearer.

What it records (§3): heart rate, steps and movement, sleep and waking, workouts and, on GPS devices, routes and locations, timestamped and continuous. **The sync chain (§4):** the watch is a relay that keeps only recent data; the phone app holds more and the manufacturer's cloud holds the full history, so the cloud account, not the watch, is usually the real source. **Preserving and extracting (§5):** the data is reached across all three, watch, phone app and cloud, with the cloud collected through the account by consent or the provider by lawful process, and preserved before app or account changes prune it.

Accuracy and attribution (§6): wearable metrics are indicative not clinical, accuracy varies, and the device is worn by whoever wore it, so findings are corroborated and stated at the level the data supports. **Deployment (§7):** activity and location timelines, testing an injury or alibi against the body's record, and the heightened UK GDPR sensitivity of health data.

- **The body keeps a log:** heart rate, steps, sleep and GPS, timestamped and near-continuous.
- **The cloud is the real source:** the watch keeps little; the full history lives in the app and the manufacturer's cloud.
- **Reach it through the account:** collected by consent or lawful process, preserved before syncing prunes it.
- **Indicative, not clinical:** accuracy varies, so wearable metrics are corroborated, not taken as medical fact.
- **Health data, handled with care:** wearable data is sensitive personal data engaging heightened UK GDPR duties.

The sync chain: sensors on the wrist, history in the cloud

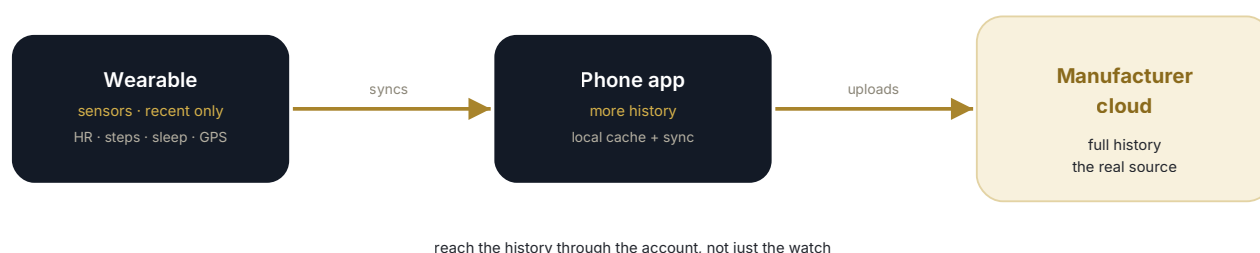


Figure 1 - the wearable is a sensor relay; the detailed activity, location and health history flows through the phone app to the manufacturer's cloud, which is usually the real evidential source.

The problem in plain English: the body keeps a log

A fitness tracker or smartwatch is worn constantly, and it measures the body continuously: how fast the heart is beating, how many steps have been taken, whether the wearer is moving or still, asleep or awake, and, if the device has GPS, precisely where an outdoor activity went. Over a day it builds a minute-by-minute record of a person's physical existence, and over months it accumulates a diary more detailed than most people keep of themselves. The important thing to understand is that very little of this stays on the watch. The watch is a small sensor and relay with limited storage; it holds recent data and then syncs it, through an app on the paired phone, up to the manufacturer's cloud, where the full history is stored and analysed. Ask for the data from the watch alone and you get a fragment; the real record is in the account.

For a lawyer this record can be unexpectedly decisive. It can show that a person was walking briskly at a time they said they were incapacitated, or asleep when they claimed to be somewhere, or on a particular route at a particular moment. It can, in the gravest cases, mark the point at which activity and heart rate ceased. But it demands care on three fronts. It is intimate health data, among the most sensitive categories the UK GDPR protects, so it must be obtained lawfully and handled with minimisation. Its accuracy is indicative, not clinical: consumer sensors estimate, and estimates can be wrong. And it records the device, not certainly the person: a watch shows what happened to whoever was wearing it, which is usually but not always its owner. This guide sets out what the wearable records, where the record lives, how to obtain it properly, and how to use it without overclaiming.

§ 0 3 · WHAT WEARABLES RECORD

What wearables record, and where the data lives

- **Activity and movement:** steps, distance, active minutes, calories and movement intensity, near-continuously through the day: a record of when the wearer was active and when at rest, timestamped.
- **Heart rate:** continuous or frequent heart-rate readings, often second by second during activity: a physiological trace that can indicate exertion, rest, stress and, at the extreme, cessation.
- **Sleep and wake:** sleep periods, stages and disturbances inferred from movement and heart rate: a record of when the wearer was asleep or awake, useful for timelines and alibis.
- **Location and routes:** on GPS-equipped devices, the routes of runs, rides and walks with times and coordinates, and sometimes continuous location: a movement record comparable to phone location (guide 124).
- **Where it lives:** the watch holds recent data only; the phone app holds more; and the manufacturer's cloud holds the full, detailed history, so the cloud account is usually the real source, reached through the account, not the device (§4).

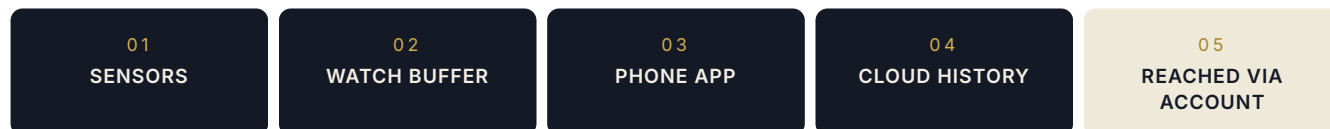


Figure 2 - the data path from wrist to cloud; the evidential weight sits at the cloud end, reached through the account rather than scraped off the watch.

The watch, the phone and the cloud: the sync chain

- **The watch as relay:** limited storage holding recent readings until they sync, so the watch alone yields only a short window and is not, by itself, the full record: useful for the most recent data and device-level artefacts, but not the history.
- **The phone app:** the companion app on the paired phone caches a fuller history and mediates the sync, holding app databases that a phone extraction can recover (guides 4, 5): a richer source than the watch, and often available where the cloud is not.
- **The manufacturer's cloud:** the full, detailed, long-term history, activity, heart rate, sleep, location, stored and analysed server-side and reached through the user's account by consent, subject-access or lawful process, or through the provider by disclosure order: the real source for anything beyond the recent window (guides 111 to 114's cloud discipline).
- **Export and subject access:** most platforms allow the user to export their own data, and a data subject can obtain their history by subject-access request, a lawful and proportionate route to a party's own wearable record (guide 20).
- **The account is the reach:** as with all synced sources, the evidence is reached through the controlling account, so identifying the account and preserving it, before it is closed, pruned or its retention lapses, matters more than possessing the watch (§5).

Preserving and extracting wearable data

- **Preserve across all three:** the watch, the paired phone and the cloud account preserved together, because each holds a different depth of the record and the fuller history is in the app and cloud, not the watch (§4): the whole chain secured, not just the device on the wrist.
- **Preserve the account promptly:** the cloud history preserved before the account is closed, the app uninstalled, retention lapses or a resync prunes local caches, an account-preservation step, like other cloud sources (guide 99's volatile-source urgency).
- **Collect the cloud lawfully:** the detailed history collected through the account by consent or subject access, or from the provider by lawful process, in a documented, reproducible way (guide 71): the real record obtained by the right route.
- **Extract the phone app and watch:** the companion app's databases recovered from a phone extraction, and the watch's recent data and artefacts extracted where they add value, with integrity preserved and hashed (guides 2, 3).
- **Minimise from the outset:** because wearable data is sensitive health data, the collection scoped to the relevant metrics and period and the rest minimised, so intimate data beyond the issue is not needlessly gathered (§7, guide 20).

Accuracy, attribution and honest limits

- **Indicative, not clinical:** consumer wearable metrics are estimates, heart rate from optical sensors, sleep inferred from movement, steps from motion, and can be inaccurate: presented as indicative evidence, corroborated, not as clinical measurement (guide 100's honest-limits discipline).
- **The device, not certainly the person:** a wearable records whoever wore it, usually the owner but not invariably: attribution corroborated, and the finding stated at the level the evidence supports, as with any device (guide 105).
- **Gaps and non-wear:** the record has gaps when the device is not worn, is charging or has synced incompletely: absence of data is not evidence of inactivity, and gaps are explained, not over-read.
- **Corroborate with other sources:** wearable data cross-checked against the phone's location and activity, messages and other evidence, so the body's record and the device record confirm each other (guide 96's timeline discipline).
- **Timing and clocks:** timestamps checked and reconciled, and the platform's own processing (how it defines a workout, a sleep period) understood before the data is read against a legal timeline (guide 108).

Deployment: timelines, injury, location and health-data sensitivity

- **Activity and injury claims:** the wearable's activity record tested against a claimed injury or incapacity, high step counts, workouts or brisk activity during a period of alleged disability, as objective evidence in personal-injury and insurance disputes (guide 98), presented as indicative and corroborated.
- **Timelines and alibis:** sleep, activity and location placing a person at rest, active or on a route at a given time, confirming or refuting an account, in criminal, family and civil matters (guide 96), with the device-not-person limit stated.
- **Location evidence:** GPS routes and locations from the wearable corroborating or contradicting other location sources, a further input to the converging location picture (guide 124).
- **The gravest cases:** in some serious matters, the cessation of heart rate and activity marking a time of death or collapse, deployed with appropriate expert and pathological context, never as a lay reading of raw data.
- **Health-data sensitivity:** wearable data is special-category health data under the UK GDPR, so its collection, disclosure and use carry heightened duties, lawful basis, minimisation, security, and the intimate data beyond the issue is protected and not needlessly exposed (§5, guide 20).

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the watch is the least important node in its own estate. The watch holds only recent data; the paired phone's companion app holds a fuller cached history; and the manufacturer's cloud holds the complete, detailed, long-term record, which is the real source. Beside these, the phone's own location and activity corroborate the wearable's; other platforms the user syncs to (a separate health aggregator, a training platform) hold copies; the counterparties and other devices (a partner's linked account, a shared challenge) may reflect the same activity; and a subject-access export gives the user's own full history lawfully. The discipline is to identify the account and preserve the cloud first, then the phone app, then the watch, in inverse order of how people instinctively reach for them, and to corroborate the body's record against the phone and the other sources rather than resting on the wearable alone. When the watch has been reset or lost, the cloud account still holds the history; when the cloud is inaccessible, the phone app's cache holds much of it; and when a party disputes their own data, their subject-access export settles what the account contains.

EVIDENCE	THE WATCH	PHONE APP CACHE	MANUFACTURER CLOUD	PHONE'S OWN DATA	OTHER PLATFORMS	DELETED / PRUNED
Activity / steps	Recent only	Y: fuller history	Y: full history	Phone motion	Aggregator copies	Cloud usually retains
Heart rate	Recent only	Y: cached	Y: detailed	n/a	Sometimes	Cloud retains
Sleep / wake	Recent	Y	Y: full	n/a	Aggregator	Cloud retains
Location / routes	Recent GPS	Y: workout routes	Y: full routes	Y: phone location	Training platforms	Varies
Account / device links	Paired identity	Account in app	Y: account records	Linked accounts	Shared challenges	Account logs

Fallback strategy in one line: preserve the cloud account first, then the phone app, then the watch; the history lives in the cloud, the app cache backs it up, and a subject-access export lawfully yields a party's own full record.

Worked examples

EXAMPLE 1 · THE ACTIVITY THAT TESTED THE INJURY CLAIM

A claimant said a workplace injury had left him largely immobile for months. His own fitness tracker told a more active story. Obtained lawfully by subject access to his account (§4), the §3 activity and location history showed, during the period of claimed incapacity, regular workouts, high step counts and several GPS-tracked runs. The §6 handling was careful: the data was presented as indicative rather than clinical, corroborated against his phone's location for the same days, and confined to the relevant metrics and period with the rest minimised as sensitive health data (§7). The report was explicit that the tracker recorded the device and that attribution to the claimant rested on corroboration, though here it was strong. The objective activity record, honestly bounded, was difficult to reconcile with the pleaded incapacity and reshaped the claim. The lesson is §7's: the body's own record can test a claim powerfully, provided it is obtained lawfully, corroborated and presented as indicative, not overstated as medical proof.

EXAMPLE 2 · THE RESET WATCH AND THE CLOUD THAT REMEMBERED

A wearable central to a timeline had been factory-reset by its user after a dispute arose, and examination of the watch itself yielded almost nothing, only recent, post-reset data, a §4 watch-as-relay limit. But the §8 estate carried the case: the detailed history had long since synced to the manufacturer's cloud, and the account, preserved before it could be closed and then collected through lawful process, held the full record of activity, heart rate and sleep for the relevant period intact, untouched by the reset of the device. The §6 timeline was reconstructed from the cloud, not the wiped watch, and the reset itself, dated after the duty to preserve had arisen, became a §10 spoliation point. The lesson is §8's: the watch is the least important node, the history lives in the cloud, and resetting the device does not reset the account.

EXAMPLE 3 · THE SLEEP RECORD THAT PLACED A PERSON AT REST

An alibi turned on whether a person had been at home asleep during a narrow window. Their smartwatch's §3 sleep and heart-rate record, obtained lawfully from the account, indicated a continuous sleep period spanning the window, low, stable heart rate and no significant movement, consistent with being asleep and at rest. The §6 limits were stated plainly: the data indicated the wearer was at rest, not certainly the account holder and not certainly at a particular place, so it was corroborated with the phone, which was also stationary at the home location, and the two together supported the alibi more honestly than either alone. The finding was expressed as indicative and corroborated, never as proof from the watch by itself. The lesson is §6's: wearable data can support an alibi, but it records a sleeping body, not an identity or a place, and its weight comes from careful corroboration and honest limits.

Common mistakes and technical limitations

Common mistakes

- **Chasing the watch, not the account:** the fundamental error, extracting the watch and missing that the full history is in the cloud (Example 2, §4).
- **Treating estimates as clinical fact:** consumer heart-rate or sleep data read as medical measurement rather than indicative estimate (§6).
- **Assuming the wearer is the owner:** the device data attributed to a person without corroboration (Example 3, §6).
- **Over-reading gaps:** absence of data (non-wear, charging) treated as evidence of inactivity (§6).
- **Ignoring the phone app:** the companion app's rich cached history overlooked where the cloud is unavailable (§4).
- **Collecting everything:** years of intimate health data swept up where a scoped, minimised period was proportionate (§5, §7).
- **Mishandling sensitive data:** special-category health data collected or disclosed without lawful basis and minimisation (§7).
- **Delay:** the account closed, the app uninstalled or retention lapsed before preservation (§5).

Technical limitations

- **Accuracy is limited:** consumer sensors estimate and can err; the data is indicative, not clinical: the honest limit, stated (§6).
- **The watch holds little:** the device is a relay; the history is in the app and cloud, not on the wrist (§4).
- **Attribution needs corroboration:** the device records the wearer, not certainly the owner or a location (§6).
- **Cloud access needs process:** the detailed history is reached through the account or provider on legal timelines (§4).
- **Platform processing is opaque:** how a platform defines a workout, sleep stage or metric affects the data and must be understood before it is relied on (§6).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What wearable devices and fitness or health apps are involved, and whose accounts hold the data, so we target the cloud, not just the watch?
- What period and which metrics (activity, heart rate, sleep, location) are relevant, so collection is scoped and minimised?
- Can the party's own history be obtained by export or subject access as a lawful, proportionate route?

Ask your opponent (or a data holder)

- Please preserve, without resetting the device, closing the account or uninstalling the app, all wearable and fitness-app data for [person] for [period], including the on-device data, the companion-app data and the full history held in the manufacturer's cloud account.
- Please disclose the relevant activity, heart-rate, sleep and location records for [period], or provide a complete data export from the account for that period.
- Please identify the wearable devices, apps and accounts involved and confirm what has been reset, deleted or exported since [date].

Ask your eDiscovery / forensic provider

- Where does the full history live for this device and platform, and how is the account collected lawfully?
- How accurate are these metrics, and how should they be corroborated and honestly bounded?
- How do we scope and minimise the collection of sensitive health data to the relevant period and metrics?

SUGGESTED WORDING · INSTRUCTION FOR A WEARABLE-DATA EXAMINATION

"We instruct you to preserve, collect and examine the wearable and fitness-app data for the person and period at Schedule 1. Please: (1) preserve the full record across the device, the companion app on the paired phone and the manufacturer's cloud account, prioritising preservation of the cloud account before it can be closed, reset or pruned; (2) collect the detailed history lawfully, through the account by consent or subject access, or from the provider by lawful process, in a documented, reproducible way, scoping the collection to the relevant metrics (activity, heart rate, sleep, location) and period and minimising other sensitive health data; (3) extract the companion-app databases and any relevant on-device data, preserving integrity; (4) present the metrics as indicative rather than clinical, explain their accuracy and any gaps, and corroborate them against the phone and other sources; and (5) state honestly that the device records the wearer, not certainly the account holder or a specific place, expressing attribution at the level the evidence supports. Treat all wearable data as special-category health data throughout."

Checklist and red flags · When to involve a digital forensic expert

The wearable-data checklist

- ☐ Devices, apps and accounts identified; cloud account located
- ☐ Cloud account preserved first, before reset, closure or pruning
- ☐ Companion-app and on-device data preserved alongside the cloud
- ☐ History collected lawfully by consent, subject access or process
- ☐ Collection scoped to relevant metrics and period; rest minimised
- ☐ Metrics presented as indicative, not clinical; accuracy explained
- ☐ Gaps and non-wear explained, not over-read
- ☐ Data corroborated against phone and other sources
- ☐ Attribution stated honestly: wearer, not certainly the owner or place
- ☐ All data treated as special-category health data under UK GDPR

Red flags

- Only the watch examined, the cloud account ignored: Example 2.
- A device reset after the dispute arose.
- Consumer metrics asserted as clinical or medical fact.
- Device data attributed to a person with no corroboration.
- Data gaps read as proof of inactivity.
- Years of intimate health data collected without scoping.
- Health data handled without lawful basis or minimisation.

When to involve a digital forensic expert

Early, to identify the account and preserve the cloud history before a reset, closure or resync prunes it, and to preserve the phone app and watch alongside (Example 2, §5); at collection, where the detailed history is obtained lawfully through the account, subject access or provider process, scoped and minimised as sensitive health data (§5, §7); at interpretation, where the metrics are presented as indicative, their accuracy and gaps explained, and the finding corroborated and honestly attributed to the wearer rather than assumed of the owner (Examples 1 and 3, §6); and at deployment, where activity, sleep and location are explained under CPR Part 35 or CrimPR Part 19, with the indicative-not-clinical and device-not-person limits made explicit and the health-data sensitivity respected. Through **cflab.uk** and **e-discovery.uk**, wearable work reaches past the watch to the account, obtains the record lawfully, and confines it honestly to what it shows: because the wearable is an intimate witness, and its evidence is only as good as the care with which it is obtained and bounded.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is the data on the watch itself?

Only recently: the watch is a relay with limited storage, holding recent readings until they sync (§4). The fuller history is cached in the companion app on the paired phone, and the complete, detailed, long-term record lives in the manufacturer's cloud, which is usually the real source (§3, Example 2). So the account, not the watch, is what you preserve and collect first; extracting the watch alone yields a fragment.

How accurate is fitness-tracker data?

Indicative, not clinical: consumer sensors estimate, heart rate optically, sleep from movement, steps from motion, and can be wrong (§6). That does not make the data useless; it makes it evidence to be presented as indicative and corroborated against other sources, not asserted as medical measurement. Its accuracy and any gaps are explained honestly, so the court knows the weight it can bear.

Does the watch prove who was doing the activity?

No, only that whoever was wearing it did (§6, Example 3). Usually that is the owner, but not invariably, so attribution requires corroboration, the paired phone's location, messages, other evidence, and the finding is stated at the level the data supports. The wearable records a body's activity; identifying whose body, and where, comes from the corroborating sources beside it.

Can we get the other side's wearable data?

By the proper routes: preservation and disclosure of the relevant records, or a data export from the account, and for a party's own data a subject-access request is often a lawful, proportionate route (§4). Because this is special-category health data, collection is scoped to the relevant metrics and period and minimised, and handled with heightened care (§7). It is obtained lawfully and proportionately, not scraped indiscriminately.

The device was reset. Is the data gone?

Usually not: a factory reset clears the watch, but the history has already synced to the cloud, and the account, preserved and collected lawfully, holds the full record untouched by the reset (Example 2, §8). Resetting the device does not reset the account. And a reset performed after the duty to preserve arose may itself be a spoliation point (§10). The wiped watch is rarely the end of the record.

Is wearable health data specially protected?

Yes: activity, heart-rate and sleep data are special-category health data under the UK GDPR, among the most sensitive personal data, so their collection, disclosure and use carry heightened duties, a lawful basis, data minimisation and security (§7). In practice this means scoping to the relevant period and metrics, protecting the intimate data beyond the issue, and handling the whole collection with the care that health information demands.

§ 1 4 · REFERENCE

Glossary

Wearable

A watch or tracker worn on the body recording activity and health.

Companion app

The phone app that syncs and caches the wearable's data.

Sync chain

The path from watch to phone app to manufacturer cloud.

Heart-rate sensor

An optical sensor estimating pulse; indicative, not clinical.

Sleep tracking

Sleep and wake inferred from movement and heart rate.

Activity data

Steps, distance, active minutes and movement intensity.

Subject access

A data subject's request for their own held data.

Special-category data

Sensitive data, including health, with heightened UK GDPR duties.

Non-wear gap

A period with no data because the device was not worn.

Indicative metric

An estimated reading, corroborated rather than taken as fact.

Sources and authoritative references

The wearable-forensics disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (wearable, companion-app and cloud health-data extraction, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (account preservation and lawful cloud collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- ICO, special-category data and health data guidance under the UK GDPR: ico.org.uk, [special-category data](https://ico.org.uk/guidance/special-category-data) · right of access: [ico.org.uk](https://ico.org.uk/guidance/right-of-access), [right of access](https://ico.org.uk/guidance/right-of-access)
- Forensic Science Regulator, Code of Practice v2: gov.uk, [FSR Code](https://gov.uk/guidance/fsr-code) · NIST SP 800-101 Rev. 1, Mobile Device Forensics (companion-app extraction principles): csrc.nist.gov, [SP 800-101](https://csrc.nist.gov/publications/sp800-101)
- PD 57AD and CPR Part 31: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd57ad) · justice.gov.uk, [Part 31](https://justice.gov.uk/cpr-part-31) · CPR Part 35: justice.gov.uk, [Part 35](https://justice.gov.uk/cpr-part-35)

DISCLAIMER

This publication provides general information about wearable and fitness-tracker forensics as at August 2026. Devices, platforms, the data they record and its accuracy vary and change; wearable metrics are indicative, not clinical, and their evidential weight depends on corroboration and context. Wearable data is sensitive health data and must be handled lawfully. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Wearable work at the laboratory starts where the evidence really lives, not on the wrist but in the account: the cloud history is identified and preserved first, before a reset, closure or resync can prune it, with the companion app and the watch preserved alongside (Example 2). The detailed record is collected lawfully, through the account by consent or subject access, or from the provider by lawful process, and scoped to the relevant metrics and period, because this is special-category health data and minimisation matters from the outset (§7). The metrics are then presented honestly: indicative rather than clinical, their accuracy and gaps explained, corroborated against the phone and other sources, and attributed to the wearer at the level the evidence supports rather than assumed of the owner or a place (Examples 1 and 3). In the gravest matters the cessation of activity and heart rate is handled with proper expert and pathological context, never as a lay reading. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and where a wearable matters, the first move is to reach past the device to the account and to obtain the intimate record lawfully, proportionately and with honest limits.



INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES

+44 (0)20 7164 6971

EMAIL

info@cflab.uk

E-DISCOVERY

e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom

cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace