Coordinated Security & Privacy Disclosure, Final Report

Samsung Health (com.sec.android.app.shealth)

Samsung Electronics Co., Ltd, Suwon, South Korea (KRX: 005930)

SILENT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 94 DAYS AFTER DISCLOSURE, THE ONLY REPLY EVER RECEIVED WAS AN AUTOMATED TICKET CLOSURE

Target	Samsung Health, pre-installed on every Galaxy device, 500 million-plus users
Package	com.sec.android.app.shealth, a 76,401-smali-class production binary
Operator	Samsung Electronics Co., Ltd, Suwon, South Korea
Initial Disclosure	2026-06-22
Original Embargo	2026-09-20 (90 days from disclosure)
Report Published	2026-09-24, four days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Austrian DSB, CERT.at
Total Outbound Messages	8, across 94 days, after three initial delivery bounces to now-dead Samsung addresses
Only Inbound Substantive Reply	2026-07-02, an automated DPO ticket-closure notice, closing the case as an unspecified request type and redirecting to a generic web form. No finding was ever named.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 22 June 2026, RFI-IRFOS disclosed to Samsung Electronics that Samsung Health, pre-installed on every Galaxy device and used by over 500 million people, declares read and write access to sixteen GDPR Art. 9 special-category health data types, including blood glucose, blood pressure, and reproductive health data, with write access capable of modifying records sourced from third-party apps such as Fitbit, Garmin, and Withings without those apps' own consent. The same binary integrates Samsung's Rubin AI behavioral-profiling engine, 926 smali classes, feeding it this same health data undisclosed in Samsung Health's own privacy policy, and separately declares CONTROL_CARE and READ_CARE permissions granting the app the ability to read and modify the health-care settings of children registered under Samsung's parental care system.

Two further CRITICAL findings: an active NFC receiver class for blood-glucose continuous-monitor data with no stated medical-device certification disclosure, and a parallel permission architecture (ChinaSettingsPermissionActivity, CHINA_NAL_PERMISSION) for PRC compliance compiled into the same globally-distributed Google Play binary, raising China National Intelligence Law Art. 7 exposure for any device that routes through it. Five HIGH findings covered undisclosed generative-AI (Gauss) processing of health data, undocumented menstrual and fertility tracking, a full installed-application inventory permission with no health purpose, background microphone access, and full contact-list and phone-number access.

Across 94 days and eight outbound messages, sent after three initial messages bounced against dead Samsung addresses, the only substantive reply Samsung ever sent was an automated Data Protection Officer notice, received 2 July 2026, closing the request as an unspecified inquiry type and redirecting to a generic consumer web form, RFI-IRFOS's own Corporate Response Pattern Atlas records this as Pattern P-01, the Webform Shuffle. No finding, of the ten disclosed, was ever named, disputed, or confirmed fixed by Samsung in any communication.

All ten findings were re-scored under CVSS v4.0 for this closure report, not carried forward with the original hand-assigned labels. Two findings, C1 (the sixteen-category read/write access) and C3 (children's care control), independently reach CRITICAL on their own CVSS math, no escalation required. C2 (Rubin AI profiling), C5 (the China permission architecture), and H2 (fertility tracking) each have a CVSS v4.0 base of MEDIUM, 6.9, and are held at HIGH in this report under explicit blast-radius escalations, documented in each finding, for a population in the hundreds of millions, standing PRC governance exposure, and a documented real-world subpoena precedent for reproductive health data respectively. H4 (background microphone) independently reaches HIGH, 8.7. C4, H1, H3, and H5 are corrected down from their original labels to match their own CVSS v4.0 bands honestly.

Scope: Root-level static analysis of the production Samsung Health Android application (com.sec.android.app.shealth), covering the AndroidManifest, resource strings, and decompiled dex, as pulled and reviewed on 22 June 2026 (76,401 smali classes). No dynamic instrumentation, live traffic capture, or interaction with Samsung's backend infrastructure was performed. RFI-IRFOS was unable to pull a fresh production build for this closure report and does not claim to know whether the ten findings still hold against the current Google Play build, that gap is stated here explicitly, it is not assumed either way.

Disposition

Ten findings were disclosed on 22 June 2026, originally labeled five CRITICAL and five HIGH; re-scored under CVSS v4.0 for this closure report, two independently reach CRITICAL (C1, broad read/write access to sixteen Art. 9 health data categories, and C3, control over children's health-care settings), three reach HIGH under explicit blast-radius escalation (C2, an undisclosed AI behavioral-profiling engine fed by health data; C5, a parallel PRC National Intelligence Law permission architecture compiled into the globally-distributed binary; H2, undocumented reproductive-health tracking), one reaches HIGH on CVSS alone (H4, background microphone access), and four correct down to MEDIUM (C4, H1, H3, H5). Eight messages were sent across 94 days. The only substantive reply, received 2 July 2026, was an automated Data Protection Officer ticket-closure notice stating the request category was unclear and redirecting to a generic web form, without naming a single finding. No further reply of any kind arrived, human or automated, apart from one out-of-office auto-response on 12 September 2026. This report closes and publishes the case on the terms disclosed from the first message.

ID	Severity	Title
C1	CRITICAL	Sixteen GDPR Art. 9 Health Categories Declared Read and Write, Including Cross-App Modification Without Source Consent
C2	HIGH	Rubin AI Behavioral-Profiling Engine Fed Undisclosed Health Data
C3	CRITICAL	CONTROL_CARE and READ_CARE, Read and Modify Access to Children's Health-Care Settings
C4	MEDIUM	Active NFC Blood-Glucose Receiver, No Stated Medical-Device Certification Disclosure
C5	HIGH	Parallel PRC National Intelligence Law Permission Architecture in the Globally-Distributed Binary
H1	MEDIUM	Samsung Gauss Generative AI Processes Health Data, Undisclosed
H2	HIGH	Menstrual Cycle and Fertility-Window Tracking, No Documented Purpose Limitation
H3	MEDIUM	QUERY_ALL_PACKAGES, Full Installed-Application Inventory
H4	HIGH	Background Microphone Access With No Documented Health Purpose
H5	MEDIUM	Full Contact List and Phone Number Access

Subject & Operator Analysis

Samsung Health is pre-installed on every Galaxy device and used by over 500 million people, operated by Samsung Electronics Co., Ltd, Suwon, South Korea, a company subject to the EU's South Korea adequacy decision (2021), which covers the lawfulness of the underlying data transfer, not the purpose-limitation and transparency findings in this report. Samsung maintains a formal DPO intake process, which in this case closed the disclosure as an unspecified request category without ever engaging a human reviewer, and an out-of-office auto-reply was the only other message this case ever received.

Several genuine positives are worth naming: no advertising SDK (no Facebook Audience Network, no ByteDance Pangle, no Adjust/AppsFlyer) is present, Samsung Health is not an ad platform. No hardcoded plaintext credential and no certificate-pinning misconfiguration was identified. These are real, and they sit alongside the findings below, not against them.

Architecture & Data Flow

The Samsung Health production APK compiles read and write access to sixteen Art. 9 health categories, an undisclosed AI behavioral-profiling engine (Rubin, 926 classes) fed by that same data, control permissions over children's health-care settings, an active NFC medical-device data receiver, and a parallel PRC-compliance permission architecture, all inside the same globally-distributed binary served through Google Play. Five further permissions (generative-AI health processing, reproductive-health tracking, a full app inventory, background microphone, and full contact access) sit alongside these without documented, narrow health purposes.

Findings

C1: Sixteen GDPR Art. 9 Health Categories Declared Read and Write, Including Cross-App Modification Without Source Consent

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3.

Samsung Health's Health Connect integration declares READ and WRITE access to sixteen Art. 9 health data categories: blood glucose, blood pressure, body fat, heart rate, oxygen saturation, VO2 max, basal metabolic rate, total calories, nutrition, exercise, sleep, distance, height, weight, speed, and power. WRITE access on categories sourced from third-party fitness platforms (Fitbit, Garmin, Withings) means Samsung Health can modify health records those platforms' own users never authorized Samsung to alter.

This finding was never disputed, confirmed, or addressed by Samsung at any point across eight messages and 94 days. The only reply received, an automated DPO ticket closure, did not engage with it.

Impact: Full read and write access to the broadest special-category health dataset RFI-IRFOS has documented in this campaign, at a scale of 500 million-plus devices, with write access reaching into records a user authorized a different company, not Samsung, to control.

Fix: Narrow WRITE access to categories Samsung Health itself originates, and require explicit, per-category consent before any cross-platform health record can be modified. No confirmation that this has occurred was ever received.

C2: Rubin AI Behavioral-Profiling Engine Fed Undisclosed Health Data

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because of the scale of the affected population, 500 million-plus devices, and because the data category involved is Art. 9 health data feeding an undisclosed behavioral-profiling system, a combination CVSS's technical vector does not on its own capture.

926 smali classes integrate Samsung's Rubin AI persona-building engine into Samsung Health, declaring READ_CONTEXT_MANAGER and READ_PERSONA_MANAGER permissions. Rubin builds a device-wide behavioral profile from continuous signals; Samsung Health, with sixteen Art. 9 categories and a continuous wearable biosensor stream, feeds this profile the most intimate data available on the device. This integration is not named or disclosed in Samsung Health's own privacy policy. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because of the scale of the affected population, 500 million-plus devices, and because the data category involved is Art. 9 health data feeding an undisclosed behavioral-profiling system.

Impact: An undisclosed AI system builds an ongoing behavioral profile of the user from their health data specifically, without the transparency GDPR Art. 13 and the automated-decision-making safeguards of Art. 22 require.

Fix: Disclose the Rubin integration by name in the Samsung Health privacy policy, specify what health signals it receives, and provide the Art. 22 safeguards that apply to any automated profiling derived from them. No confirmation that this has occurred was ever received.

C3: CONTROL_CARE and READ_CARE, Read and Modify Access to Children's Health-Care Settings

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3.

Samsung Health declares CONTROL_CARE and READ_CARE permissions, granting the app the ability to read the health data of children registered under Samsung's parental care system and to modify their care settings. Children's health data under GDPR Art. 8 carries the highest protection category in the regulation, and no health-tracking purpose in a general consumer app requires the ability to control a minor's parental care settings from within it.

Impact: Read and write access to a child's health data and care configuration, held by a general fitness and wellness application with no documented, narrow purpose for that specific capability.

Fix: Remove CONTROL_CARE and READ_CARE from Samsung Health, or restrict them to a narrowly scoped, separately consented parental-control feature with its own Art. 8 safeguards. No confirmation that this has occurred was ever received.

C4: Active NFC Blood-Glucose Receiver, No Stated Medical-Device Certification Disclosure

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 5.2. Corrected from the original CRITICAL label under CVSS v4.0, the access path requires NFC proximity, it is not remotely exploitable, and no demonstrated exploitation beyond the declared capability was ever established.

TrackerBloodGlucoseNfcDataReceiver is active in the production binary, combined with android.permission.NFC and READ_BLOOD_GLUCOSE/WRITE_BLOOD_GLUCOSE. This constitutes an active medical-device data pipeline, continuous glucose monitors such as Abbott FreeStyle Libre and Dexcom transmit diagnostic data via NFC, with no MDR 2017/745 certification disclosure found in Samsung Health's privacy policy.

Impact: A functioning medical-device data ingestion path exists in production without a disclosed compliance basis under the EU Medical Device Regulation, though exploitation requires physical NFC proximity to the source device, not a remote attack path.

Fix: Publish the MDR 2017/745 certification or compliance basis covering this data pipeline. No confirmation that this has occurred was ever received.

C5: Parallel PRC National Intelligence Law Permission Architecture in the Globally-Distributed Binary

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the same binary, carrying this permission architecture, is distributed to the entire 500 million-plus global user base through the standard Google Play channel, not a China-specific build.

ChinaSettingsPermissionActivity and a CHINA_NAL_PERMISSION intent declare a parallel permission flow for PRC compliance, compiled into the same binary served globally via Google Play. Samsung devices used in China, or by Chinese travelers carrying the app in the EU, may route health data under PRC Cybersecurity Law Art. 37 and National Intelligence Law Art. 7. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the same binary, carrying this permission architecture, is distributed to the entire 500 million-plus global user base through the standard Google Play channel, not a China-specific build.

Impact: A compiled, PRC-compliance-specific code path exists in the identical binary every global user receives, without Samsung ever confirming, when asked, whether this path is a durable build-time exclusion for non-China users or a remotely configurable flag.

Fix: Confirm and publish whether the China-specific permission flow is compiled out of non-China builds or gated by a verifiable, durable technical control. No confirmation that this has occurred was ever received.

H1: Samsung Gauss Generative AI Processes Health Data, Undisclosed

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. Corrected from the original HIGH label under CVSS v4.0.

A GENAI_RECLAIM code path processes health data through Samsung's Gauss generative AI models, with no disclosure in the privacy policy that generative AI performs this processing. GDPR Art. 13 requires transparent disclosure of automated processing, including AI-assisted analysis, of this kind.

Impact: Health data is processed by a generative AI model the user is never told about, foreclosing any informed decision about whether to allow that specific processing.

Fix: Name the Gauss integration explicitly in the privacy policy and describe what health data it processes. No confirmation that this has occurred was ever received.

H2: Menstrual Cycle and Fertility-Window Tracking, No Documented Purpose Limitation

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because reproductive health data of exactly this kind has already been subpoenaed in real criminal investigations, a documented real-world consequence CVSS's technical vector does not capture.

CYCLE_RECORD_PERIOD and CYCLE_REMAINDER_FERTILE_WINDOW track menstrual cycle and fertility-window data. No documented purpose limitation or third-party sharing policy specific to this data category was found in Samsung Health's privacy policy, despite reproductive health data's distinct, heightened legal exposure since the Dobbs decision in the United States. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because reproductive health data of exactly this kind has already been subpoenaed in real criminal investigations, a documented real-world consequence CVSS's technical vector does not capture.

Impact: Reproductive health data, a category with a documented history of legal subpoena in criminal proceedings, is collected without a stated, category-specific purpose limitation or sharing policy.

Fix: Publish a category-specific purpose limitation and third-party sharing policy for menstrual and fertility data, distinct from general health metrics. No confirmation that this has occurred was ever received.

H3: QUERY_ALL_PACKAGES, Full Installed-Application Inventory

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. Corrected from the original HIGH label under CVSS v4.0.

Samsung Health declares QUERY_ALL_PACKAGES, enumerating every application installed on the device. No health-tracking purpose requires a complete inventory of installed applications, a GDPR Art. 5(1)(c) data-minimization gap.

Impact: The full list of a user's installed applications, itself a behaviorally revealing dataset, is available to Samsung Health with no documented health-related justification.

Fix: Remove QUERY_ALL_PACKAGES or narrow it to the specific package names Samsung Health actually needs to interoperate with. No confirmation that this has occurred was ever received.

H4: Background Microphone Access With No Documented Health Purpose

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

RECORD_AUDIO combined with FOREGROUND_SERVICE_MICROPHONE grants background microphone access. Combined with a health-monitoring app running persistently in the foreground, audio capture with no documented health purpose is a significant confidentiality exposure independent of any other finding in this report.

Impact: A persistently running health app holds the technical capability to capture ambient audio in the background, with no health use case in Samsung's own documentation explaining why.

Fix: Remove background microphone access or publish the specific, narrow health feature it supports and confine the permission to active use of that feature only. No confirmation that this has occurred was ever received.

H5: Full Contact List and Phone Number Access

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. Corrected from the original HIGH label under CVSS v4.0.

READ_CONTACTS, READ_PHONE_NUMBERS, and READ_PHONE_STATE together grant access to the full contact list and phone number inventory. No health-tracking use case documented by Samsung requires this scope of access.

Impact: A user's complete social graph, via their contact list, is available to a health app with no stated health-related purpose for that access.

Fix: Remove contact and phone-state permissions, or narrow them to the specific, documented feature that requires them (for example, emergency contact selection) with a runtime, feature-scoped request. No confirmation that this has occurred was ever received.

Impact Analysis

The findings compound, they do not sit side by side as isolated issues. C1 establishes the broadest possible read/write surface over the most sensitive data category GDPR defines. C2 shows that surface feeds an undisclosed AI profiling system. C3 shows the same surface extends to children. H2 and H4 show the surface is not even limited to health metrics in the narrow sense, reproductive data and ambient audio both sit inside the same application, at the same scale, under the same undisclosed governance.

Pattern P-01, The Webform Shuffle

The single substantive reply this case ever received, an automated DPO ticket closure on 2 July 2026, is documented in the RFI-IRFOS Corporate Response Pattern Atlas v0.1 as Pattern P-01, the Webform Shuffle: a formal, technical, regulator-BCC'd disclosure routed into a consumer-facing request-category form, closed for lacking a category selection the form was never designed to hold, and redirected to a generic web intake with no record of the original findings attached. No human reviewer at Samsung is known to have read any of the ten findings.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 9(1)(2)	C1	Read and write processing of sixteen special-category health data types, including cross-platform modification without source-app consent.
Art. 9, Art. 13, Art. 22	C2	Undisclosed automated profiling of health data by an AI behavioral engine.
Art. 8, Art. 9	C3	Children's health data is the highest-protection category in the regulation; no documented purpose justifies app-level control over care settings.
Art. 9, MDR 2017/745	C4	A functioning medical-device data pipeline with no disclosed regulatory certification basis.

Article	Finding	Basis
Art. 44	C5	International transfer exposure via a PRC-compliance code path compiled into the globally-distributed binary.
Art. 5(1)(b), Art. 9	H2	Purpose limitation for a legally sensitive reproductive-health data category.

Regulatory & Legal Landscape

Samsung Electronics Co., Ltd is incorporated in South Korea, covered by the EU-South Korea adequacy decision (2021) for the lawfulness of the underlying transfer mechanism, a point this report does not dispute. The purpose-limitation, transparency, and children's-data findings above sit independently of that adequacy decision. The Austrian DSB and CERT.at were held in BCC across this case's correspondence from the first message.

IOC / Reproducible Evidence

```
Package: com.sec.android.app.shealth
Binary size: 76,401 smali classes

C1: HealthConnect READ+WRITE, 16 categories, incl. blood glucose, blood pressure,
    sleep
C2: 926 Rubin AI classes, READ_CONTEXT_MANAGER + READ_PERSONA_MANAGER
C3: CONTROL_CARE + READ_CARE permissions
C4: TrackerBloodGlucoseNfcDataReceiver + NFC + READ/WRITE_BLOOD_GLUCOSE
C5: ChinaSettingsPermissionActivity + CHINA_NAL_PERMISSION
H1: GENAI_RECLAIM (Samsung Gauss)
H2: CYCLE_RECORD_PERIOD + CYCLE_REMAINDER_FERTILE_WINDOW
H3: QUERY_ALL_PACKAGES
H4: RECORD_AUDIO + FOREGROUND_SERVICE_MICROPHONE
H5: READ_CONTACTS + READ_PHONE_NUMBERS + READ_PHONE_STATE
```

No fresh production build was pulled for this closure report. The findings above are reproducible against the build reviewed on 22 June 2026; RFI-IRFOS does not claim to know whether the current Google Play build still matches it, and states that gap explicitly instead of assuming continuity.

Disclosure Timeline & Outcome

Date	Event
2026-06-22	R1 sent to privacy@samsung.com , bounced. Same day, resent to s ecurity@samsungmobile.com, also bounced.
2026-06-23	R1 resent to presse@samsung.de, bounced, and eu.privacy@samsung .com, bounced. Ten findings, three questions, 90-day embargo set for 2026-09-20 (originally stated 09-19 in the R1 body, corrected to the later AUDIT_META date per RFI-IRFOS's own never-publish-earlier-than-ann ounced rule).
2026-06-27	Follow-up successfully delivered to m obile.security@samsung.com and dat aprotection.seg@samsung.com after prior bounces.
2026-07-02	Only substantive reply of the case: an automated DPO ticket closure, unspecified request category, redi- rected to a generic web form.
2026-07-27 through 2026-09-12	Five further follow-ups sent, each unanswered except one out-of-office auto-response.
2026-09-20	Original 90-day embargo elapses. No human reply had ever been received.
2026-09-24	Case closed and published, four days after embargo, on the terms stated from the first message.

Eight outbound messages across 94 days, one automated ticket closure, zero human replies, zero findings named by Samsung at any point.

Residual Risk & Recommendations

All ten findings remain unconfirmed as fixed at the time of publication, because Samsung never substantively engaged with any of them. RFI-IRFOS recommends, in order of urgency: narrow WRITE access on cross-platform health categories to require explicit per-category consent (C1); disclose the Rubin AI integration by name (C2); restrict or remove CONTROL_CARE and READ_CARE (C3); publish the MDR compliance basis for the NFC glucose pipeline (C4); confirm whether the China permission architecture is a build-time exclusion or a remote flag (C5); and apply data-minimization to the app-inventory, microphone, and contact permissions (H3-H5). Weekly monitoring of the public build continues after this publication; any change to any of the ten findings will be documented and added to the public record.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. Any such escalation is always stated explicitly in the finding itself, never left implicit, as C2, C5, and H2 are escalated and C4, H1, H3, and H5 are corrected down in this report. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF SAMSUNGHEALTH-2026-R1.