NHS
South East Coast Ambulance Service
NHS Foundation Trust

Trust Headquarters
Nexus House
4 Gatwick Road
Crawley
West Sussex
RH10 9BG

Tel: 0300 123 0999
www.secamb.nhs.uk

30th January 2026
Internal Ref: 251205
Email:

Dear ,

The trust acknowledges receipt of your Freedom of Information Act 2000 (FOIA) request, referenced above. Please ensure you quote this number in any future correspondence.

Please accept the Trust's apologies for the delay and inconvenience you have experienced regarding your FOIA request.

FOI Request & FOI Response

You asked us:

SECTION A – Contract & Commercial Information (Priority 1)
For your current ePCR solution, please provide the following:

A1. Supplier & Contract Details
- **Name of the current supplier.**

The Trust is withholding this information under **Section 31(1)(a)** of the Freedom of Information Act 2000.

"For security reasons, the Trust does not disclose the names of specific systems, suppliers, technologies, or detailed system configurations in response to FOI requests. Releasing this level of technical detail would be likely to prejudice the prevention or detection of crime by exposing information that could be exploited to identify vulnerabilities, target the organisation's infrastructure, or compromise cybersecurity controls. Disclosure would therefore increase the risk of malicious activity and undermine the Trust's ability to protect its critical systems and data."

The Trust is also applying a **Section 24** Exemption – National Security, to this request.

Section 24(1) allows a public authority not to disclose information if you consider that releasing the information would make the UK or its citizens more vulnerable to a national security threat.

Network and Information Systems (NIS) Regulations 2018 includes healthcare as services critical to the economy and wider society, to which Section 24 exemption applies.

While there is a general public interest in transparency and accountability, this is outweighed by the strong public interest in maintaining the security and resilience of NHS systems that support clinical operations, patient care, and organisational infrastructure. Disclosing such information would place these services at increased risk of cyberattack, which would not be in the public interest.

- **Contract reference number (where applicable).**

ecm_14713

- **Contract start date, initial end date, and all extension options available.**

Contract start date was 6th September 2024 for an initial 24-month period with an option to extend for a further 1-year period.

- **Whether any extensions have already been exercised, and the updated end date.**

Extension has not been exercised as of yet

- **Total contract value, including any exercised extensions.**

£1,320,000 if the extension is exercised.

- **Annual contract value or recurring annual charges.**

£440,000 per annum

- **Pricing model used (e.g., per-user licence, per-device licence, per-incident, enterprise licence).**

Fixed Cost

- **Volume metrics underpinning the contract (e.g., number of operational staff, number of devices, number of ePCR submissions per year).-**

Not Applicable

A2. Scope of Services Included in the Contract
Please confirm whether the contract includes the following, and if so, provide details:

Software & Support

- **1st/2nd/3rd line support model, including operating hours and SLAs**

- 24/7 Support:

Fault Category	Description	Action	Escalation
Emergency (P1)	System is unusable or Operation is severely impacted	1hr response. Fixed withing 4hrs. Customer kept informed of progress	Technical Director advised if not fixed within 4hrs
Urgent (P2)	Important features not working or omissions in application which does not render the system unusable or generate corrupt data	2hr response. Fixed within 6hrs.Customer kept informed of progress	Technical Director advised if not fixed within 8hrs
Limited Impact (P3)	Any events which are considered an inconvenience rather than a restriction	4hr response. Fixed within 35hrs	Technical manager monitors progress.
Non Urgent/Cosmetic (P4)	Recognised as a minor fault but causing no inconvenience	7hr response. Fixed within 3 months	Technical manager monitors progress.

- **Hosting, cloud infrastructure or on-premise components included**

On premise, all components are replicated across two sites and hosted on resilient server infrastructure.

- **Application updates & release management**

One major release per annum. Excluding bug fixes.

- **Uptime requirements / contractual service levels**

On premise, expected 99.999% uptime. Supplier SLA above.

Hardware & Device Support (if applicable)

- **Supply, warranty, or lifecycle management for tablets or mobile devices**

Standard Apple support plus in house support.

- **Mobile Device Management (MDM) solution included**

Not included in EPCR contract

- **Whether rugged cases, vehicle docking, or peripheral hardware is included**

None included in EPCR contract

Vehicle Installation & Equipment Support

- **Installation/fitting of ePCR-related hardware in vehicles**
    - No EPCR equipment installed in vehicles
- **Ongoing maintenance of any vehicle-mounted equipment**

Not Applicable

- **Whether installation was carried out directly by the supplier or subcontracted**

Not Applicable

Mobile Network & Connectivity

- **Mobile network providers used for ePCR operation (e.g., EE, O2, Vodafone, multi SIM, roaming SIMs)**

Multinetwork Three SIM

- **Whether mobile network services are included in the contract or procured separately**

Not part of the EPCR contract

- **Any bandwidth management, APN, or private network arrangements**None

Mobile Data Usage

- **Approximate monthly or annual mobile data usage attributable to the ePCR (e.g., GB per device or total Trust usage, if held)**
    - Unable to split data types out as devices are COPE, average monthly download is approximately 7TB/month

<u>SECTION B – Contractual Documentation (Priority 2)</u>
For your current ePCR solution, please provide:

- **A copy of the signed contract, including all schedules, appendices and specifications.**

This information is withheld under the following exemptions:

Section 41 – Information Provided in Confidence

Contract schedules and appendices contain supplier owned proprietary information provided to the Trust under an explicit duty of confidence. Disclosure would constitute an actionable breach of confidence.

Section 43(2) – Commercial Interests

Disclosure of contractual detail, pricing structures, and variation documents would likely prejudice both the commercial interests of the supplier and the Trust's position in future procurements.

A summary of the contract is provided in Section A; however, the detailed documents themselves cannot be released.

- **Copies of any contract variations or change control notices (CCNs) relating to:**
    - **functional scope**
    - **licensing or cost changes**
    - **hardware refreshes**
    - **service level changes**

- **Any documented cost-of-change assumptions used during the procurement or contract negotiation phase.**

SECTION C – Procurement Process & Evaluation (Priority 3)
For the procurement that led to your current ePCR system, please provide:

C1. Procurement Route

- **Procurement route used (Open, Restricted, Framework, Direct Award, Further Competition).**

Direct Award via Framework

- **If a framework was used, please confirm the framework name, lot and call-off reference.**

G Cloud 13 (Ref RM1557.13)

C2. Tender Documentation. Procurement was carried out via the G-Cloud filtering portal and once a number of search criteria had been entered, G-Cloud returned one supplier as meeting the criteria.

- **Full technical specification and requirements used during tendering.**

Not Applicable

- **Any annexes, security or hosting requirements, functional requirements, user stories, or evaluation guidance.**

Not Applicable

- **Any pre-market engagement documents (PIN, soft-market testing materials) where held.**

Not Applicable

C3. Evaluation Outcomes

- **List of all bidders.**

  See above responses

- **Full evaluation criteria and weighting breakdown.**

Not Applicable

- **Scoring summary for all bidders, including:**
  - **Technical score**
  - **Commercial score**
  - **Overall score**

Not Applicable

- **Evaluator comments or narrative assessment notes.**

Not Applicable

SECTION D – Technical Architecture, Interoperability & Security (Priority 4)

D1. Monitor/Defibrillator Integration (Interoperability)

- **Current defibrillator/monitor vendor(s) used operationally.**

Stryker LifePak15

- **Integration method with the ePCR (e.g., Bluetooth, cable, serial feed, cloud-mediated, proprietary integration).**

Not currently available between monitor and ePCR platform

- **Whether vital-signs data is transferred device-to-device, via a mobile app, or through a cloud API.**

Not Applicable see above – entered manually

- **Any known limitations (e.g., iOS Bluetooth restrictions, Android compatibility issues).-**

Logistic manage these devices but they do not link to our iPads for EPCR

D2. Endpoint Security, MDM & Compliance
Please confirm the following for ePCR-related mobile devices (tablets, ruggedised devices, etc.):

- **Whether Microsoft Advanced Threat Protection / Defender for Endpoint is used.**

The Trust is withholding this information under **Section 31(1)(a)** of the Freedom of Information Act 2000.

"For security reasons, the Trust does not disclose the names of specific systems, suppliers, technologies, or detailed system configurations in response to FOI requests. Releasing this level of technical detail would be likely to prejudice the prevention or detection of crime by exposing information that could be exploited to identify vulnerabilities, target the organisation's infrastructure, or compromise cybersecurity controls. Disclosure would therefore increase the risk of malicious activity and undermine the Trust's ability to protect its critical systems and data."

The Trust is also applying a **Section 24** Exemption – National Security, to this request.

Section 24(1) allows a public authority not to disclose information if you consider that releasing the information would make the UK or its citizens more vulnerable to a national security threat.

Network and Information Systems (NIS) Regulations 2018 includes healthcare as services critical to the economy and wider society, to which Section 24 exemption applies.

While there is a general public interest in transparency and accountability, this is outweighed by the strong public interest in maintaining the security and resilience of NHS systems that support clinical operations, patient care, and organisational infrastructure. Disclosing such information would place these services at increased risk of cyber-attack, which would not be in the public interest.

If not, please confirm the alternative endpoint protection solution.

- **MDM or mobile security platform used (e.g., Intune, AirWatch, MobileIron, Samsung Knox).**

The Trust is withholding this information under **Section 31(1)(a)** of the Freedom of Information Act 2000.

"For security reasons, the Trust does not disclose the names of specific systems, suppliers, technologies, or detailed system configurations in response to FOI requests. Releasing this level of technical detail would be likely to prejudice the prevention or detection of crime by exposing information that could be exploited to identify vulnerabilities, target the organisation's infrastructure, or compromise cybersecurity controls. Disclosure would therefore increase the risk of malicious activity and undermine the Trust's ability to protect its critical systems and data."

The Trust is also applying a **Section 24** Exemption – National Security, to this request.

Section 24(1) allows a public authority not to disclose information if you consider that releasing the information would make the UK or its citizens more vulnerable to a national security threat.

Network and Information Systems (NIS) Regulations 2018 includes healthcare as services critical to the economy and wider society, to which Section 24 exemption applies.

While there is a general public interest in transparency and accountability, this is outweighed by the strong public interest in maintaining the security and resilience of NHS systems that support clinical operations, patient care, and organisational infrastructure. Disclosing such information would place these services at increased risk of cyberattack, which would not be in the public interest.

- **Minimum OS version requirements and patch/update policies.**

The Trust is withholding this information under **Section 31(1)(a)** of the Freedom of Information Act 2000.

"For security reasons, the Trust does not disclose the names of specific systems, suppliers, technologies, or detailed system configurations in response to FOI requests. Releasing this level of technical detail would be likely to prejudice the prevention or detection of crime by exposing information that could be exploited to identify vulnerabilities, target the organisation's infrastructure, or compromise cybersecurity controls. Disclosure would therefore increase the risk of malicious activity and undermine the Trust's ability to protect its critical systems and data."

The Trust is also applying a **Section 24** Exemption – National Security, to this request.

Section 24(1) allows a public authority not to disclose information if you consider that releasing the information would make the UK or its citizens more vulnerable to a national security threat.

Network and Information Systems (NIS) Regulations 2018 includes healthcare as services critical to the economy and wider society, to which Section 24 exemption applies.

While there is a general public interest in transparency and accountability, this is outweighed by the strong public interest in maintaining the security and resilience of NHS systems that support clinical operations, patient care, and organisational infrastructure. Disclosing such information would place these services at increased risk of cyberattack, which would not be in the public interest.

- **Update window requirements (e.g., iOS must be updated within X weeks of release).**

Update window requirement is in line with the trust security policy

D3. Hosting & System Architecture

- **Hosting model (SaaS, cloud, private cloud, on-premise).**
    - Hybrid, on premise plus vendor hosted
- **Cloud provider (if applicable).**

The Trust is withholding this information under **Section 31(1)(a)** of the Freedom of Information Act 2000.

"For security reasons, the Trust does not disclose the names of specific systems, suppliers, technologies, or detailed system configurations in response to FOI requests. Releasing this level of technical detail would be likely to prejudice the prevention or detection of crime by exposing information that could be exploited to identify vulnerabilities, target the organisation's infrastructure, or compromise cybersecurity controls. Disclosure would therefore increase the risk of malicious activity and undermine the Trust's ability to protect its critical systems and data."

The Trust is also applying a **Section 24** Exemption – National Security, to this request.

Section 24(1) allows a public authority not to disclose information if you consider that releasing the information would make the UK or its citizens more vulnerable to a national security threat.

Network and Information Systems (NIS) Regulations 2018 includes healthcare as services critical to the economy and wider society, to which Section 24 exemption applies.

While there is a general public interest in transparency and accountability, this is outweighed by the strong public interest in maintaining the security and resilience of NHS systems that support clinical operations, patient care, and organisational infrastructure. Disclosing such information would place these services at increased risk of cyberattack, which would not be in the public interest.

Any documented disaster recovery or failover arrangements.

The Trust is withholding this information under **Section 31(1)(a)** of the Freedom of Information Act 2000.

"For security reasons, the Trust does not disclose the names of specific systems, suppliers, technologies, or detailed system configurations in response to FOI requests. Releasing this level of technical detail would be likely to prejudice the prevention or detection of crime by exposing information that could be exploited to identify vulnerabilities, target the organisation's infrastructure, or compromise cybersecurity controls. Disclosure would therefore increase the risk of malicious activity and undermine the Trust's ability to protect its critical systems and data."

The Trust is also applying a **Section 24** Exemption – National Security, to this request.

Section 24(1) allows a public authority not to disclose information if you consider that releasing the information would make the UK or its citizens more vulnerable to a national security threat.

Network and Information Systems (NIS) Regulations 2018 includes healthcare as services critical to the economy and wider society, to which Section 24 exemption applies.

While there is a general public interest in transparency and accountability, this is outweighed by the strong public interest in maintaining the security and resilience of NHS systems that support clinical operations, patient care, and organisational infrastructure. Disclosing such information would place these services at increased risk of cyberattack, which would not be in the public interest.

SECTION E – Training, Adoption & Deployment (Priority 5)
For your current ePCR system:

- **Structure of training provided to staff (classroom, online, LMS/SCORM modules).**
    - Training for the Trust's current electronic Patient Care Record (ePCR) system is delivered face-to-face in a classroom environment. All new clinicians attend a half-day Operational Readiness session which includes the use of an ePCR device in test mode. The session covers system navigation, core functionality, and scenario-based completion exercises.
- **Duration of training for frontline clinicians.**
    - The initial Operational Readiness ePCR training delivered to all new clinicians is half a day.
- **Any refresher or ongoing training requirements.**
    - The Trust does not operate a formal, scheduled refresher programme specifically for ePCR. However, ongoing support is provided through:
        - Intranet-based video resources
        - The ePCR user manual
        - Sessions embedded within the 2025/26 Statutory & Mandatory Training curriculum
- **Copies of training materials, user guides, quick reference guides or onboarding packs (redacted if necessary).**

  See ePCR User Guide v2.1 document
- **Whether training was provided by the supplier, Trust staff, or a blended model.**

Training for the current ePCR system is delivered by the Trust's Education Department.

SECTION F – Organisational & Operational Information (Priority 6)
(For context only)

- **Total number of clinical staff (FTE or headcount).-**
- **Total number of tablets or mobile devices used for ePCR across the Trust**

Circa 3,500 iPads

SECTION G – Collaborative Procurement (Priority 7)

- **Any shared purchasing arrangements, consortia, or joint procurements the Trust participates in relating to ePCR.**

None

- **Details of any call-offs or shared contracts awarded through these arrangements.**

None

Next steps

Please note you will be able to source additional information which is made available on our website.

Should you be dissatisfied with our response then in the first instance please contact Richard Banks, Head of Corporate Governance, via the following email address: FOI@secamb.nhs.uk

You can ask us to review our original response. If you would like us to carry out an internal review, please let us know within 40 working days of you receiving our original response. This review will be conducted by an individual who was not directly involved in reviewing the original response, ordinarily, the Trust Data Protection Officer.

We will endeavour to complete this request within 20 working days.

Should you remain dissatisfied then you can contact the Information Commissioner's Office (ICO). Complaints to the ICO should be made within six weeks of receiving the outcome of an internal review. The easiest way to lodge a complaint is through their website: www.ico.org.uk/foicomplaints.

Alternatively, the ICO's postal address is:
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF.

Yours sincerely,

Freedom of Information Coordinator
South East Coast Ambulance Service NHS Foundation Trust