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

1st April 2026
Internal Reference: 260315
Email:

Dear ,

Thank you for your request for information, which we received on **04/03/2026**.
We have considered your request under the Freedom of Information Act 2000.
Please ensure you quote the Internal Reference number above in any future correspondence.

Your Request

Under the Freedom of Information Act 2000, please provide the following recorded information held by your organisation regarding assurance processes for software based data erasure of end of life IT equipment.

For clarity, this request relates specifically to the erasure of storage media associated with end of life hardware such as laptops, desktops, servers, storage arrays, or other data bearing IT equipment. It does not relate to operational deletion of data within live systems, routine account management, or DSP Toolkit self assessment processes.

Physical destruction methods such as shredding, crushing, degaussing, or disintegration are outside the scope of this request. This request concerns software based erasure only.

This request seeks to distinguish between confirmation that an erasure process was carried out and recorded evidence demonstrating that the final data state of a specific storage device is irrecoverable. I am not seeking technical configuration detail or security sensitive information, only the recorded assurance basis relied upon when concluding that personal data has been rendered irrecoverable.

Please confirm:

1) Whether your organisation's policies, contractual terms, or internal procedures require an explicit outcome based warranty or guarantee that personal data on a specific storage device has been rendered irrecoverable as a final data state following software based erasure.

2) Where software based erasure of storage media is undertaken internally, what recorded evidential assurance is relied upon to conclude that the final data state of the specific storage device is irrecoverable, as distinct from confirmation that an erasure process was executed.

3) Where software based erasure is undertaken by a third party provider:

a. Do the certificates or contractual documents held constitute an explicit outcome based warranty or guarantee of irrecoverability for each specific storage device processed?

b. Beyond reliance on supplier accreditation or recognised standards including but not limited to ADISA certification, ISO accreditation, NIST alignment, HMG IA standards, NHS Digital guidance, or Data Security and Protection Toolkit assertions, and beyond confirmation that a wiping process was completed, does the organisation hold any recorded, device specific documentation evidencing independent verification, testing, or validation that the data on the storage media has been rendered irrecoverable in practice?

4) If no explicit outcome based warranty or device specific outcome evidence is held beyond certification, accreditation, or confirmation of process completion, please confirm what recorded form of evidential assurance is relied upon when concluding that personal data has been rendered irrecoverable.

Formal Response

1. The Trust's policies, contractual terms, and internal procedures do not require an explicit outcome-based warranty or guarantee stating that personal data on a specific storage device has been rendered irrecoverable as a final data state following software-based erasure.
   Instead, the Trust relies on process-based assurance, supported by recognised standards, contractual obligations, and supplier assurances, to conclude that personal data has been rendered irrecoverable in accordance with data protection legislation and NHS guidance.

2. The Trust does not undertake large-scale internal software-based erasure of end-of-life data-bearing storage media as a routine activity.
   Where any internal erasure activity is undertaken, the recorded assurance relied upon consists of: confirmation that an approved erasure process was executed in line with Trust policy and procedural controls; and asset

management and disposal records demonstrating that the device was processed in accordance with approved information governance and security arrangements.
The Trust does not hold device-specific, outcome-based evidence demonstrating independent verification or testing that the final data state of a specific storage device is irrecoverable beyond confirmation that the approved process was completed.

3. Answers to a),b) and c):

   Software-based erasure is not undertaken by a third-party provider so the Trust does not hold certificates or contractual documents that constitute an explicit outcome-based warranty or guarantee of irrecoverability for each specific storage device.

   In line with recognised standards (such as industry or NHS guidance), and following confirmation that the erasure process has been completed, the Trust does not hold device-specific records demonstrating independent verification, testing, or validation that data on individual storage devices has been rendered irrecoverable in practice.

   The Trust does not receive or retain forensic-level validation reports or post-erasure data recovery testing evidence for individual devices

4. Where no explicit outcome-based warranty or device-specific irrecoverability evidence is held, the Trust relies on the following recorded forms of assurance when concluding that personal data has been rendered irrecoverable: Governance oversight through information asset owners and asset disposal records; compliance with Trust information governance, data protection, and asset management policies; contractual obligations requiring suppliers to apply recognised destruction standards and controls; supplier confirmations or certificates evidencing that the approved destruction process was completed and organisational assurance derived from audit, risk management, and compliance frameworks. This assurance model reflects the Trust's current recorded position and is consistent with wider NHS practice and regulatory expectations.

Next steps

Some information held by the Trust is routinely published on our website and may be of assistance.

If you are dissatisfied with the Trust's response to your request, you have the right to ask for an internal review.

Requests for an internal review should be submitted within **40 working days** of the date of this response and should be sent to:

Richard Banks, Head of Corporate Governance at **FOI@secamb.nhs.uk**

The internal review will be conducted by an individual who was not directly involved in handling your original request, ordinarily the Trust's Data Protection Officer. We aim to complete internal reviews within **20 working days** of receipt.

If you remain dissatisfied following the outcome of the internal review, you may complain to the Information Commissioner's Office (ICO). The ICO generally expects complaints to be raised promptly following the completion of an internal review.

The easiest way to raise a complaint is via the ICO's website:
www.ico.org.uk/foicomplaints

Alternatively, you may write to:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Yours sincerely,

Corporate Governance Team
South East Coast Ambulance Service NHS Foundation Trust