

FOI 3673

1st April 2026

FREEDOM OF INFORMATION ACT 2000 – INFORMATION REQUEST

- 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.**

Response:

The Trust does not operate an outcome based warranty. Trust data is cleansed from devices as part of device destruction process. Evidence of erasure/ destruction is returned to the Trust.

- 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.**

Response:

The Trust does not undertake internal software based erasure of storage media.

- 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?**

Response:

Yes

- 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?**

Response:

Software based erasure is undertaken via approved contractors operating on HSCNI certified frameworks.

- 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.

Response:

All HSC data is wiped prior to removal from Trust site or as part of device destruction contracted process. Evidence of erasure/ destruction is returned to the Trust in the form of a 'Data Destruction Certificate'.

Email: Foi.Team@Southerntrust.hscni.net