Northern Health and Social Care Trust

FOI 3828

Recorded Assurance 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.

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.

Contractual terms include the provision of certificate confirming the that the erasure process was carried out and confirming the nature of the erasure process (e.g. software wiped or permanent shredding) against the specific device asset number (if relevant).

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.

N/A as erasure is carried out as part of an external service.

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?

Contractual terms include the provision of certificate confirming the that the erasure process was carried out and confirming the nature of the erasure process (e.g. software wiped or permanent shredding) against the specific device asset number (if relevant).

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?

No - We hold only the certificate from the provider confirming that the erasure process was carried out and confirming the nature of the erasure process (e.g. software wiped or permanent shredding).

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.

We hold only the certificate from the provider confirming that the erasure process was carried out and confirming the nature of the erasure process (e.g. software wiped or permanent shredding).