

27/03/2026

NN-ICB/26-1534

Dear Requestor

Re: Freedom of Information Request

Thank you for your request for information, received on 4 March 2026, regarding recorded assurance for software based data erasure of end of life IT equipment. We have processed your request in accordance with the Freedom of Information Act 2000 (FOIA).

Under the FOIA, public authorities like ours are required to respond to requests for information within 20 working days. In response to your request, I can confirm that we do hold the information requested.

Please find below our response to your request:

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.

Nottinghamshire Health Informatics Service (NHIS) undertakes the management of end of life equipment as part of the IT contract held with Nottingham and Nottinghamshire Integrated Care Board. This is in connection with both ICB corporate and Primary Care/GP devices.

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.

NHIS disposal and decommission procedures do require a guarantee that patient, personal and / or organisational data on any storage device has been irrecoverably cleared during the software based data erasure stage. This process is always conducted within NHIS premises and no data device leaves their site without undergoing the full data erasure process.

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.

The data erasure software overwrites the storage device with new data patterns so the original data cannot be recovered, which makes the data permanently unrecoverable.

The software employed also has a number of national and international accreditations including: ISO/IEC 15408 / ISO 27001, 27701 and 14001 / ADISA Product Assurance / CESG (former UK Government Information Security Authority - part of GCHQ).

The adopted software also complies with major security standards, i.e.: NIST SP 800-88 / IEEE 2883 / HIPAA / GDPR.

Once data erasure has been completed, each device is issued with a Data Destruction Certificate which remains permanently accessible for reference at any time.

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?

Yes. Each device is issued with a Data Destruction Certificate which remains permanently accessible for reference at any time. These certificates are issued as a means to provide NHS / ICB with a guarantee that the data has irrecoverably been erased.

- 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?

Once data erasure has been completed, each device is issued with a Data Destruction Certificate which remains permanently accessible for reference at any time and guarantees that the data has been permanently and irrecoverably removed / wiped.

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.

Not applicable.

If you are unhappy with the way in which your request has been handled, NHS Nottingham and Nottinghamshire Integrated Care Board (ICB) has an internal review procedure through which you can raise any concerns you might have. Further details of this procedure can be obtained by contacting Lucy Branson, Director of Corporate Governance and Assurance via lucy.branson@nhs.net or by writing to FOI Team at NHS Nottingham and Nottinghamshire ICB, Sir John Robinson House, Sir John Robinson Way, Arnold, Daybrook, Nottingham NG5 6DA.

If you remain dissatisfied with the outcome of the internal review, you can apply to the Information Commissioner's Office (ICO), who will consider whether the organisation has complied with its obligations under the Act and can require the organisation to remedy any problems. Generally, the ICO cannot make a decision unless you have exhausted the complaints procedure provided by NHS Nottingham and

Nottinghamshire ICB. You can find out more about how to do this, and about the Act in general, on the Information Commissioner's Office website at: <https://ico.org.uk/for-the-public/>.

Complaints to the Information Commissioner's Office should be sent to:

FOI/EIR Complaints Resolution, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone 0303 123 1113 or report a concern via <https://ico.org.uk/concerns/>.

Yours sincerely

Freedom of Information (FOI) Officer on behalf of NHS Nottingham and Nottinghamshire Integrated Care Board nnicb-nn.foi@nhs.net

All information we have provided is subject to the provisions of the Re-use of Public Sector Information Regulations 2015. Accordingly, if the information has been made available for re-use under the [Open Government Licence](#) (OGL) a request to re-use is not required, but the license conditions must be met. You must not re-use any previously unreleased information without having the consent of NHS Nottingham and Nottinghamshire Integrated Care Board. Should you wish to re-use previously unreleased information then you must make your request in writing (email will suffice) to the FOI Lead via nnicb-nn.foi@nhs.net. All requests for re-use will be responded to within 20 working days of receipt.