

Freedom of Information Act 2000

The Royal Cornwall Hospitals NHS Trust Response to Information request

Date Request Received: 29th July 2025

FOI Ref No 29742

Requested Information:

1. Does your organisation currently use or maintain any of the following legacy Oracle systems?

- Oracle 8
- Oracle 9i
- Oracle Forms (any version)

This information would be held by your CIO or CTO in the IT department and CFO in the Finance Department.

2. If so, please provide:

- a. The name and version of the system(s)
- b. The department(s) or function(s) using the system
- c. Whether there are any planned upgrade or decommissioning projects in place
- d. The name and role of the responsible officer (e.g., CIO, CTO, CFO)

Response:

The NHS organisation can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here: <http://www.legislation.gov.uk/ukpga/2000/36/section/31>

S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.

As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

Factors in favour of confirming or denying the information is held

The NHS organisation considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the NHS Trust's ICT infrastructure and would reveal details about the Trust's information security systems. The NHS organisation recognises that answering the request

would promote openness and transparency with regards to the NHS Trust's ICT security.

Factors in favour of neither confirming nor denying the information is held

Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. The NHS Trust, like any organisation, may be subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, the NHS organisation considers that confirming or denying whether the requested information is held would provide information about the NHS Trust's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the NHS Trust's information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

If the NHS organisation were either to confirm or deny the existence of the requested information, the disclosure would be likely to prejudice, the effective conduct of public affairs for the Trust, the NHS or any other government department(s) and as such conflicts with Section 36(2c) of the FOIA. The full wording of section 36 can be found here: <https://www.legislation.gov.uk/ukpga/2000/36/section/36>

Balancing the public interest factors

The NHS organisation has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extent the NHS organisation is able to detect and deal with ICT security attacks. The NHS Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the NHS Trust's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the NHS Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the NHS organisation being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have,

which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the NHS Trust's operations including its front-line services. The prejudice in complying with section 1(1)(a) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the NHS Trust's ICT system

Attachment(s):

No Attachment(s)

Date Response sent: 19th August 2025