Northern Health and Social Care Trust

FOI 3815

Computer Aided Facilities Management Systems

Q1. What software does your Trust currently use for its CAFM (Computer Aided Facilities Management) solution?
If multiple systems are in use, please list all solutions rather than only the primary system.

Information relating to the identity of the software and its supplier is withheld. Please refer to below exemption.

Q2. What is the contract expiry date for the software used?
If the contract is annual or rolling, please state this. If multiple systems are in use, please provide the known expiry date (or contract term details) for each.

October 2026

Q3. Who is the person responsible for managing this system?

Mr M McKernan

Q4. What is that person's job title?

Asset & Estates Information Manager

Exemption and Public Interest Test

The Trust is mindful that any disclosure of information under FOI legislation is to the world at large and not just to the person who submitted the request. This has been taken into account when deciding on the release of information in response to an FOI request, giving due consideration to the exemptions preventing disclosure of certain information into the public domain.

The Trust has feels that this information meets the requirement for exemption under Section 43 (Disclosure would pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the NHSCT relies).

In order to engage the exemption, the Trust must demonstrate that there is a causal link between the endangerment and disclosure of the information and that disclosure would or would be likely to have, a significant threat to the integrity and operation of the digital systems on which the day to day business of NHSCT relies. The threat cannot be trivial or insignificant.

In recent years, there have been a number of Cyber Attacks on public authorities, where the perpetrators may have exploited vulnerabilities in ICT systems and software to gain access and either deploy ransomware or steal information. In May 2021 the Health Service in Ireland (HSE) suffered such an attack and in light of this, the Trust is mindful that by releasing information about the digital infrastructure and devices connected to its ICT network (which may also be electronically linked to other healthcare organisations in Northern Ireland), it could reveal versions of systems/software/quantities/contacts which may be exploitable and would enable access to its wider ICT network.

This would endanger the information it holds on patients, clients and staff and the loss of this information would directly impact on the physical or mental health wellbeing of those patients and clients, as the Trust would not have access to key information for continuity of their care. Given the HSE ransomware attack, the actual risk of a remote attack on the Trust's ICT network is real, substantial and probable.

For this reason the Trust will not be releasing details of the Trust's cyber security operational practices and processes as has been requested within this FOI request as this has the potential to increase the likelihood for a remote attack on our ICT systems.

Section 43 – Public Interest Test

Section 43 is a qualified exemption. This means that, as information requested is exempt from disclosure, the Trust consider and then decide whether the public interest in maintaining the exemption outweighs the public interest in its disclosure. In the case of section 43 this involves weighing up the threat to the integrity & operation of the digital systems on which the day-to-day business of the NHSCT relies and the potential impact on health and safety to patients, clients and staff against any public interest in disclosure.

The assessment of endangerment is relevant to this public interest test as the Trust believes this information would be of use to perpetrators and the impact of such an attack would be substantially detrimental for our patients and clients. Due to the level and likelihood of endangerment, the Trust is convinced there is a very strong public interest in not disclosing the information requested and the Section 43 exemption is fully engaged.

EXEMPTION CLAIMED IN RESPECT OF SECTION 43 **Integrity & operation of the digital systems**	
In favour of disclosure of information	**In favour of maintaining exemption and not disclosing information**
The Trust's desire for openness, fairness, transparency and equity.	There have been a number of cyber-attacks against health care and public sector organisations across the UK and ROI, which demonstrates a strong risk to the NHSCT's ICT Systems.
Transparency in accountability of public funds and ensure public money is being used effectively. Provide assistance to the public in understanding where and how public monies are spent.	The Trust holds highly sensitive information on our patients and clients and the loss (even temporarily) of this information would impact on the Trust's ability to deliver services and provide medical and social care.
To ensure procurements and contracts are conducted and managed in an open and honest way.	There would be a detrimental impact on the mental health and wellbeing of our clients (and patients) if there data was compromised or stolen.
Ensuring there is competition for public sector contracts.	The Trust may be liable to regulatory action or a monetary penalty if information was released into the public domain (via FOIA) which contributed to identifying vulnerabilities in our ICT systems and ultimately led to or contributed to remote cyber-attack.
	Release of the information in light of the potential impact may undermine public confidence in the Trust.
	A potential cyber-attack will endanger the Trust's wider ICT systems, further

	compromising its ability to deliver services.
	A Cyber-attack may impact upon other health trusts who use the same regional systems and place supplier/contracting organisations at risk.