Scope

FOI requests seeking information regarding core digital infrastructure incl hardware, software, systems, designs, processes, planning, resourcing, risks, existing contracts and security incidents.

Overview

Disclosure of information about Belfast Trusts core digital infrastructure would put the Trusts digital infrastructure under elevated levels of security risk and become more vulnerable to a malicious cyber security attack.

The disclosure of such information would:
a) (Section 31) Leave Belfast Trust, Patients, Clients & Staff more vulnerable to crime;
b) (Section 38) Be likely to endanger the safety, or the physical or mental health of individuals within Belfast Trust
c) (Section 43) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the Trust relies

Section 31 – Law Enforcement

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

- To protect the work of one that does
- To withhold information that would make anyone, including the public authority itself, more vulnerable to crime

Factors in Favour of Disclosure	Factors Against Disclosure
Principle that there is public interest in transparency and accountability in disclosing information about public sector procedures, contracts and purchasing.	Disclosure of this information would leave the Trust more vulnerable to crime, with the crime in question being malicious attack on the Trusts infrastructure and systems. Information security across the HSC is of critical importance to delivery of care, protection of information assets and many related business processes. If a Cyber incident should occur, without effective security and controls, HSC information, systems and infrastructure may become unreliable, not accessible when required (temporarily or permanently), or compromised by unauthorised 3rd parties including criminals. This could result in unparalleled HSC-wide disruption of services due to the lack of/unavailability of systems that facilitate HSC services (e.g. appointments, admissions to hospital, ED attendances, checking critical registers) or data contained within. This may result in the need to cancel appointments and treatments, or divert emergency/essential clinical or other services. The significant business disruption could also lead to increased waiting lists, delayed urgent clinical interventions, suboptimal clinical or social care outcomes and potentially bring liabilities for the Service. It could also lead to unauthorized access to any of our systems or information (including clinical/medical systems), theft of information or finances, breach of statutory obligations, substantial fines and significant reputational damage.

Section 38 – Health & Safety

Section 38 states that information is exempt if its disclosure could lead to the physical or mental harm of, or endanger the safety of, individuals.

Disclosure of the requested information would leave the Belfast Trusts digital infrastructure at significant risk of cyber security attack. A cyber-security attack may lead to the placing of sensitive health & social care information into the public domain and, as such, the Trust believes there is a link between the risk of endangerment for data subjects and the disclosure of the requested information. There would likely be a substantial detrimental effect on the physical or mental health of patients, clients, staff or their families should the requested information be released.

Factors in Favour of Disclosure	Factors Against Disclosure
Principle that there is public interest in: • Transparency and accountability in how the Trust safeguards health & social care data and uses its resources. • Transparency and accountability in disclosing information about public sector procedures, systems, contracts and use of public funds.	Disclosure of this information would leave the Trust more vulnerable to cyber security attack which would likely endanger or lead to a breach of sensitive health & social care information about patients, clients or staff. It would also lead to significant damage and costs to recover information, systems or infrastructure. The public exposure or disclosure of sensitive information would lead to significant distress for individuals and their families, particularly those who are already vulnerable, and in some cases lead to individuals or their families becoming targets based on their health conditions or circumstances. There is a public expectation on the Trust to keep their information confidential and secure, as well as legal obligations such as a duty under Data Protection Act 2018 to safeguard public information.

Section 43 – Commercial Interests

Section 43(2) states that information is exempt if its disclosure would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it).

Disclosure of the requested information would leave the Belfast Trusts digital infrastructure at significant risk of cyber security attack. This would compromise the Belfast Trusts ability to provide Health & Social Care Services and carry on business-as usual should the digital systems be compromised.

Factors in Favour of Disclosure	Factors Against Disclosure
Strong interest in disclosure of information that informs the public about how we spend our money. Principle that there is public interest in transparency and accountability in disclosing information about public sector procedures, contracts and purchasing.	Disclosure of this information would prejudice/damage the Trusts commercial interests and potentially disclose information which would allow an insight into the Trust security model and behaviours, and that of the wider HSCNI. This would leave the Trusts digital infrastructure at risk of malicious attack. Information security across the HSC is of critical importance to delivery of care, protection of information assets and many related business processes. If a Cyber incident should occur, without effective security and controls, HSC information, systems and infrastructure may become unreliable, not accessible when required (temporarily or permanently), or compromised by unauthorised 3rd parties including criminals. This could result in unparalleled HSC-wide disruption of services due to the lack of/unavailability of systems that facilitate HSC services (e.g. appointments, admissions to hospital, ED attendances, checking critical registers) or data contained within. This may result in the need to cancel appointments and

	treatments, or divert emergency/essential clinical or other services. The significant business disruption could also lead to increased waiting lists, delayed urgent clinical interventions, suboptimal clinical or social care outcomes and potentially bring liabilities for the Service. It could also lead to unauthorized access to any of our systems or information (including clinical/medical systems), theft of information or finances, breach of statutory obligations, substantial fines and significant reputational damage

There is an overwhelming public interest in keeping Health & Social Care digital systems and critical national infrastructure secure which would be served by non-disclosure. This outweighs the public interest in accountability and transparency which would be served by disclosure.