Belfast Health and Social Care Trust
caring supporting improving together

FOI/34826

17 October 2025

IT Program Supplier Information

1. Digital Dictation	
• **Name of supplier & product**	Information withheld on basis of cyber threat
• **Number of user licences**	Information withheld on basis of cyber threat
• **Procurement method (e.g., framework)**	Information withheld on basis of cyber threat
• **Contract start date**	Information withheld on basis of cyber threat
• **Contract expiry date (please specify fixed end date vs option to extend/rolling contract)**	Information withheld on basis of cyber threat
• **Total contract value (if available)**	Information withheld on basis of cyber threat
• **Integration with PAS/EPR (please specify if outbound only – e.g., patient demographics, clinic work list – or outbound and inbound, e.g., document return)**	Information withheld on basis of cyber threat
• **Key internal stakeholder role/title**	Information withheld on basis of cyber threat
• **Desired features not currently delivered (optional)**	Information withheld on basis of cyber threat

2. Outsourced Transcription	
• **Name of supplier & product**	Information withheld on basis of cyber threat
• **Procurement method (e.g., framework)**	Information withheld on basis of cyber threat
• **Contract start date**	Information withheld on basis of cyber threat
• **Average monthly volume of letters (if available)**	Information withheld on basis of cyber threat
• **Average monthly volume of lines (if available)**	Information withheld on basis of cyber threat

• **Total contract value (if available)**	Information withheld on basis of cyber threat
• **Key internal stakeholder role/title**	Information withheld on basis of cyber threat
• **Desired features not currently delivered (optional)**	Information withheld on basis of cyber threat

3. Speech Recognition

• **Name of supplier & product**	Information withheld on basis of cyber threat
• **Number of user licences**	Information withheld on basis of cyber threat
• **Procurement method (e.g., framework)**	Information withheld on basis of cyber threat
• **Contract start date**	Information withheld on basis of cyber threat
• **Contract expiry date (please specify fixed end date vs option to extend/rolling contract)**	Information withheld on basis of cyber threat
• **Total contract value (if available)**	Information withheld on basis of cyber threat
• **Integration with PAS/EPR (please specify if outbound only – e.g., patient demographics, clinic work list – or outbound and inbound, e.g., document return)**	Information withheld on basis of cyber threat
• **Key internal stakeholder role/title**	Information withheld on basis of cyber threat
• **Desired features not currently delivered (optional)**	Information withheld on basis of cyber threat

4. Ambient AI Scribe

• **Name of supplier & product**	Information withheld on basis of cyber threat
• **Number of user licences**	Information withheld on basis of cyber threat
• **Procurement method (e.g., framework)**	Information withheld on basis of cyber threat
• **Contract start date**	Information withheld on basis of cyber threat

• **Contract expiry date (please specify fixed end date vs option to extend/rolling contract)**	Information withheld on basis of cyber threat
• **Total contract value (if available)**	Information withheld on basis of cyber threat
• **Integration with PAS/EPR (please specify if outbound only – e.g., patient demographics, clinic work list – or outbound and inbound, e.g., document return)**	Information withheld on basis of cyber threat
• **Pilot stage (if applicable, please specify supplier, pilot duration, and scope)**	Information withheld on basis of cyber threat
• **Key internal stakeholder role/title**	Information withheld on basis of cyber threat
• **Desired features not currently delivered (optional)**	Information withheld on basis of cyber threat

5. Video Consultation

• **Name of supplier & product**	Information withheld on basis of cyber threat
• **Number of user licences**	Information withheld on basis of cyber threat
• **Procurement method (e.g., framework)**	Information withheld on basis of cyber threat
• **Contract start date**	Information withheld on basis of cyber threat
• **Contract expiry date (please specify fixed end date vs option to extend/rolling contract)**	Information withheld on basis of cyber threat
• **Total contract value (if available)**	Information withheld on basis of cyber threat
• **Integration with PAS/EPR (please specify if outbound only – e.g., patient demographics, clinic work list – or outbound and inbound, e.g., document return)**	Information withheld on basis of cyber threat
• **Key internal stakeholder role/title**	Information withheld on basis of cyber threat
• **Desired features not currently delivered (optional)**	Information withheld on basis of cyber threat
• **Average number of video appointments per month/year**	Information withheld on basis of cyber threat

• **% of virtual/remote consultations conducted using video vs telephone**	Information withheld on basis of cyber threat

6. Health Information Systems

• **PAS (Patient Administration System)**	Information withheld on basis of cyber threat
• **EPR (Electronic Patient Record)**	Information withheld on basis of cyber threat
• **eDMS (Electronic Document Management System)**	Information withheld on basis of cyber threat
• **RIS (Radiology Information System)**	Information withheld on basis of cyber threat
• **LIMS (Laboratory Information Management System)**	Information withheld on basis of cyber threat
• **e-Correspondence (e.g., Docman)**	Information withheld on basis of cyber threat
• **Hybrid Mail (e.g., Synertec, Healthcare Communications)**	Information withheld on basis of cyber threat
• **Patient Portal (e.g., Patient Knows Best)**	Information withheld on basis of cyber threat

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:

- (Section 31) Leave Belfast Trust, Patients, Clients & Staff more vulnerable to crime;
- (Section 38) Be likely to endanger the safety, or the physical or mental health of individuals within Belfast Trust
- (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 To protect the work of one that does

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:

- Protect the work of one that does

- To Withhold information which would make anyone, including the public authority itself, more vulnerable to crime

Section 28 – Health and 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.

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.