Belfast Health and Social Care Trust
caring supporting improving together

FOI/28996

31 March 2023

Palantir Technologies

1. Does your organisation use Palantir software for any purpose or policy?

2. If so please state the name of the software, the date on which use commenced, and the purposes and policies for which it is used.

3. Do you upload patient data to to Palantir e.g. Foundry? Please state the name of this data, the policy under which it is uploaded, and whether it is "de-identified", "pseudonymised" or anonymised.

4. Have you conducted data protection impact assessments on your use of Palantir? Please provide a copy of these impact assessments if so.

If you use Palantir software:

5. Please provide copies of correspondence between relevant employees of your organisation and employees of Palantir related to the implementation and usage of - and troubleshooting issues with - Palantir software.

Please define correspondence as emails, text messages and WhatsApp messages generated since 01/06/2022.

6. Please provide copies of internal correspondence related to the implementation and usage of - and troubleshooting issues with - Palantir software.

Please define internal correspondence as emails generated since 01/06/2022.

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) leave Belfast Trust, Patients, Clients & Staff more vulnerable to crime (Section 31);
b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the Trust relies (Section 43).

The information requested is therefore exempt from release under the following Sections of the Freedom of Information Act 2000.

31 March 2023

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

The exemption is subject to the public interest test. There is an overwhelming public interest in keeping Health & Social Care digital systems secure which would be served by non-disclosure. This outweighs the public interest in accountability and transparency which would be served by disclosure.

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 & Care Services and carry on business-as usual should the digital systems be compromised.

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