FOI 060/2021 Response

Request

Dear Birmingham and Solihull Mental Health NHS Foundation Trust,

Please pass this on to the person who conducts Freedom of Information reviews.

I am writing to request an internal review of Birmingham and Solihull Mental Health NHS Foundation Trust's handling of my FOI request 'Information regarding Darktrace'.

The Trust declined to confirm whether it was using Darktrace in May 2017. The basis of that refusal was that there would be some risk to the Trust's cybersecurity if such disclosures were made. The Trust cites exemption Section 24, which requires the Trust to show that there would be a "causal" link between the disclosures and the alleged harms.

The Trust in its refusal has not made such a showing. The Trust states simply that "disclosure of the requested information would compromise the Trust's ICT security and leave our servers vulnerable to cyber-attacks." It does not explain its position further.

My request did not relate to the Trust's current ICT security. My request sought only the basic fact of whether the Trust used a particular supplier some four years ago, long in the past. This is of no use to a potential hacker today. Even the most skilled hackers cannot go back in time to attack the Trust, and information about a state of affairs years in the past does not reveal anything about the current status of the Trust's cybersecurity systems. You will be aware that May 2017 was the month the WannaCry attack hit the NHS -- I don't think anybody thinks that NHS cybersecurity defences did not change following that incident.

For these reasons, I do not believe that the Trust can make the required showing of a casual link to harm under the cited exemption

Response

The Trust is of firm opinion that your request for information in relation to Darktrace has been appropriately responded too.

The Trust is of the stance that all requests for information that pertain to security products or services, whether past or present will not be disclosed.

This is because disclosure of the information has the potential to leave the Trust's systems compromised and vulnerable as we may deploy similar or reinstate previously used security services or products.