File reference	W17FOI293
Key words	Contacts and cybercrime
Date of release	21/06/2017
Attachments	No

Freedom of Information Act Disclosure log - Reply Extract

File Reference: **17FOI293**

Date request received: **22/05/2017**

Disclosure due date: **21/06/2017**

Disclosure date: **14/06/2017**

……..

Freedom of Information Act 2000 – Response
I refer to your email received 22/05/2017 in which you requested information under the terms of the Freedom of Information Act 2000. Plymouth Hospitals NHS Trust is confirming in accordance with section 1 (a) of the Act that it holds the information requested and is supplying it in accordance with section 1(b) unless otherwise specified.

For organisational context: Plymouth Hospitals NHS Trust is the largest teaching hospital trust in the South West. We employ over 6,900 staff working in 350 different roles within the Trust. We offer a full range of general hospital services to around 450,000 people in Plymouth, North and East Cornwall and South and West Devon. These include emergency and trauma services, maternity services, paediatrics and a full range of diagnostic, medical and surgical sub-specialties.

We work within a network of other hospitals to offer a range of specialist services to a population of between 700,000 and two million depending on the type of care needed.

"Contact us" details are available on the Trust website at http://www.plymouthhospitals.nhs.uk/contact-us. This includes an online enquiry form.

You asked

1. **The name and job title of your current clinical chief information officer(s) (CCIO)**

2. **The name and job title of your current clinical safety officer(s) (CSO)**

3. **Were any computers, tablets, mobile devices at your trust affected by the recent Ransomware (WannaCry) 'attack'?**

a. If yes, was any patient data lost (e.g. progress notes, pathology results, radiology results, medication history etc.)? Please specify what data was lost and over what time frame.

4. If you were not affected the ransomware, did you limit/prevent clinical staff access to computers/other devices as a precaution?

5. Do you utilise a managed service for cybersecurity, or manage it internally using commercial off the shelf (COTS) solutions?

b. If a managed service – please can you name the provider?

c. If COTS solution – please can you name all the products used?

Our response

Q1 = The Trust's Clinical Chief Information Officer(s) (CCIO) is

Dr P Hughes – Medical Director is the CCIO.

Q2 = The Trust's Clinical Safety Officer(s)(CSO) is

Mr S Brundell - Consultant Colorectal Surgeon Lead.

Q3 to 5 = Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply to these questions.

Our legal statement relating to the use of exemptions

Introduction

Section 31 and 38 apply to questions three to five. We are sorry that we cannot be more helpful, but trust that you will understand our approach in light of the risks associated with responding, particularly in light of recent national news events about cybercrime.

We have for some time adopted a similar approach to all requests about our integrated network security and believe this is necessary in maintaining the highest levels of security.

Exemptions applied

Section 31.-(1) (a) the prevention or detection of crime applies, as does 31.-(3) neither confirming nor denying we hold the information requested.

Section 38-(1) (a) and (b) the Health and Safety exemption applies. Additionally section 38.-(2) applies in that we are neither confirming nor denying we hold the information requested.

Exemptions use rationale

This disclosure would prejudice the prevention and detection of crime and any information, albeit confirming what we hold or do not hold could assist criminals and place our patients and staff at harm. The Trust has provided a more detailed rationale below for each exemption used and applied them following the careful consideration of submissions made to a Public Interest Test in deciding the outcome of our response to you.

Section 31 – Law enforcement- prevention of crime

We consider this exemption applies because disclosing details of our security arrangements could prejudice the security and integrity of the Trust's network and increase the risk of unauthorised access to information held by the Trust, much of which is confidential and sensitive. The level of detail that would be released would enable external parties, who are not privy to the confidential aspects of Trust's IT systems, knowledge of our security equipment and by association its integrated network security. The Trust employs a range of security tools to mitigate the risk from different types of security threats. Firewalls, Intruder Detection Devices Antivirus and other products form a mesh of security that protects the Plymouth NHS Network and data, the more of these vectors that are known, the weaker the security of the network protection. There is a real risk that this knowledge could assist external parties in attempting a cyber-attack/hack into the Plymouth NHS Network. The anticipated harm from this is a breach of data protection (failure to protect information resulting in an unauthorised disclosure), data loss, and disruption to patient care through a loss of IT services. The severity of harm is extensive with millions of patient records put at risk of unauthorised disclosure.

Section 38 Health and Safety

Such disclosures also endanger the physical or mental health and safety of patients and staff. The dangers have become self-evident from recent events reported in the news, including delays to treatment and diagnostics to name but a few. Any failure of our infrastructure endangers both the physical and mental health of our patients and exposes them to danger.