Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI/LHCH/2017078
From: Commercial

Date: 15 March 2017

Subject: Cyber security

Q1 Has your organisation completed all of the government's '10 steps to cyber security'?

A1 Yes

Q2 Have you suffered Distributed Denial of Service (DDoS) cyber attacks on your network in the last year?

A2 No

Q3 If so, how many DDoS attacks did you experience during 2016?

A3 Information not held – as A2 above

Q4 Has your organisation ever been the victim of a DDoS attack which was used in combination with another type of cyber attack, such as a demand for ransom/ransomware, network infiltration or data theft?

A4 Information not held – as A2 above

Q5 How does your IT team detect that your organisation has suffered a DDoS attack?

A5 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack from hackers if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Q6 Does your method of DDoS mitigation detect sub-saturating DDoS attacks of less than 30 minutes in duration, which do not typically overwhelm the network?

A6 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information

systems and other related assets at risk of attack from hackers if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.