Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI/LHCH/2017129
From: Commercial

Date: 23 May 2017

Subject: WannaCry ransomware attack

Q1 The name and job title of your current clinical chief information officer(s) (CCIO)

A1 Our CCIO is our Medical Director – see information available on our website: https://www.lhch.nhs.uk/about-lhch/our-board-of-directors/dr-raphael-perry-deputy-chief-executive-and-medical-director/

Q2 The name and job title of your current clinical safety officer(s) (CSO)

A2 Information not held - currently no such role assigned

Q3 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.

A3 No

Q4 If you were not affected the ransomware, did you limit/prevent clinical staff access to computers/other devices as a precaution?

Q4 Information exempt under Section 38: Health and Safety. 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 potentially lead to disruption of services and/or cause harm to patients.

We can however confirm that the Trust has business continuity processes in place to cover major incidents.

Q5 Do you utilise a managed service for cybersecurity, or manage it internally using commercial off the shelf (COTS) solutions?

a. If a managed service – please can you name the provider?
b. If COTS solution – please can you name all the products used?

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.