St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	073230517
From:	Commercial
Date:	23/05/2017
Subject:	WannaCry Attack

REQUEST

Please may I request the following information?

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?

RESPONSE

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

    Rowan Pritchard Jones – Consultant Burns and Plastics Surgeon

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

Craig Walker – Information Governance Manager

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?

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information above would highlight any vulnerability, should any such vulnerability exist (within hardware or software or architecture or Vendor, etc.), within our IT infrastructure which could be exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust.

This information relating to the cyber security agenda is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

Our patients (and staff) must have confidence that their very sensitive personal data will be held securely.

They (patients & staff) must have confidence that we'll be able to provide the services they need.

Therefore, providing the specific requested information would put their confidence at risk.

Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

And therefore, this would be extremely harmful to the public & the services the Trust provides.

Therefore in accordance with Section 31 of the Freedom of Information Act the Trust will not be releasing the requested information as this would prejudice our ability to resist cyber-attacks.