St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	141070717
From:	Press
Date:	07/07/17
Subject:	Wannacry Impact

REQUEST

1) Was your trust affected by the WannaCry ransomware cyber attack on the NHS in May 2017 (http://www.bbc.co.uk/news/health-39899646) ?

2) If so, please list the hospitals or addresses of other sites within your trust affected.

3) How many outpatient appointments were cancelled or postponed because of the attack (if relevant)? Please state the number of cancellations and postponements per day, eg 12 May 2017, 13 May 2017 etc, that were as a result of the attack.

4) How many operations were cancelled or postponed because of the attack (if relevant)? Please state the number of cancellations and postponements per day, eg 12 May 2017, 13 May 2017 etc, that were as a result of the attack.

5) What was the total cost to your trust of the attack? Please break down the cost in terms of cancelled or postponed appointments, staff overtime, IT support or other expenses.

6) Did your trust pay any ransom? If so, how much was paid?

7) How many computers were affected?

8) How many computers do you have in total?

9) Did your trust install a patch to protect systems from WannaCry, issued by NHS Digital on 17 March, 25 April, 27 April and 12 May? When was it installed?

RESPONSE

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.