

Ref no: 080260517  
From: Commercial  
Date: 26/05/2017  
Subject: WannaCry HSJ

## REQUEST

Dear Sir/Madam

I hereby request under the Freedom of Information Act, the following information from your organisation.

I am sending this on Behalf of Ben Heather from HSJ

1. Did your trust shut down any IT systems in response to the ransomware attack, known as WannaCry, on or after 12 May, 2017?
2. How many computers/servers/devices infected in the ransomware attack, known as WannaCry, on 12 May, 2017?
3. How many planned appointments and/or operations did the trust cancel/postpone/reschedule as a result, either direct or indirect, of the WannaCry ransomware attack?
4. Did you trust put in place any emergency ambulance diverts from its emergency department as a result of the Wannacry ransomware attack?
5. How many "serious incidents" occurred at your trust as a result, direct or indirect, of the Wannacry ransomware attack?
6. Was there any other impact on clinical care, for example delays or lack of access to tests?
7. In 14 March, 2017, Microsoft released a patch for computers/servers/devices to remove the specific vulnerability. This was made available to trusts by NHS Digital on 25 April, 2017, and trusts were explicitly informed of this availability on 27 April, 2017. On May 12, 2017, had your trust applied the patch detailed above to all computers/server/devices running a version of Windows to which the patch was applicable?

Any additional information/insights not covered by the below questions about the response to the cyber-attack at your trust would be most welcome.

## 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.