



Information Governance

18 Mole Business Park
Leatherhead
Surrey KT22 7AD

Tel: 01372 216059

Fax: 01372 217114

Email: IGTeam@sabp.nhs.uk

18 May 2018

ID Number – FOI 4575

Title: IT Ransomware

I am now in a position to respond to your request; please see our response below:

Trust Response:

Question:	Trust Response:
Trust Name	Surrey and Borders Partnership NHS Foundation Trust
Organisational Code	RXX
Did your trust shut down any IT systems in response to the ransomware attack, known as WannaCry, on or after 12 May, 2017?	No.
How many computers/servers/devices infected in the ransomware attack, known as WannaCry, on 12 May, 2017?	None.
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?	None.
Did you trust put in place any emergency ambulance divers from its emergency department as a result of the Wannacry ransomware attack?	Not applicable.
How many "serious incidents" occurred at your trust as a result, direct or indirect, of the Wannacry ransomware attack?	None.
Was there any other impact on clinical care, for example delays or lack of access to tests?	Yes.

[For a better life](#)

Question:**Trust Response:**

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 further comments