

ion Set	Topic	Question	Answer	Details
1	Electronic patient records	Do you use an electronic patient record system? If so, please provide the name of the system(s) used?	No	The Trust has a core Patient administration system, DXC's iPM, but there is no joined up or central electronic patient record system.
		Do you use any additional electronic patient record systems for particular specialities or particular tasks? If so, please detail all the additional systems and what they are used for?	Yes	The Trust has 100s of clinical systems containing patient data, the detail information you require would take a significant amount of time to collect - This would breach the 18-hour limit
		Do you use an electronic system for documents (such as clinic letters)? If so, please detail the system(s) used?	Yes	Bighand- GP Letters; CRIS for Imaging Reports/ letters
		Do you use an electronic system for prescribing drugs? If so, please detail the system(s) used?	Yes	The Trust has just procured Marand's Open EP system with implementation imminent.
		Do you use an electronic system for patient management or administration? If so, please detail the system(s) used?	Yes	iPM (DXC)
		Do you use paper notes for any part of your clinical records? If so, please detail what aspect(s) of patient records are recorded on paper?	Yes	99% is still paper, but the Trust is just beginning to roll out 'eNotes' and we should see a significant change to electronic notes over the next couple of years.

		Do you use an electronic system for requesting and reviewing results of diagnostic tests (such as blood tests)? If so, please detail the system(s) used?	Yes	iCM (DXC)
2	Diagnostic data	Do you use an electronic system for viewing radiological and nuclear imaging? If so, please detail the system(s) used?	Yes	Picture Archive and Communications System, AWS, CMR42, Terareco
		Do you use an electronic system for recording and monitoring vital signs (such as temperature, blood pressure)? If so, please detail the system(s) used?	No	N/A
		Do you have a password protection policy for user accounts? If so, please detail what it consists of in terms of lower case, upper case and special characters?	N/A	Information Security exemption applied to response
3	Passwords	Can users change their user account password? If so, please detail how often it must be changed?	N/A	Information Security exemption applied to response
		Do users require additional passwords to log into any of the IT systems listed above? If so, which systems require additional passwords?	N/A	Information Security exemption applied to response
		How many desktop or portable computers are currently managed by the trust? (An estimate is sufficient)		6500

4	Security	Are there desktop or portable computers running Microsoft Windows XP or Microsoft Windows Vista in the trust? If so, please detail how many of each? (An estimate is sufficient)	N/A	Information Security exemption applied to response
		Are all desktop and portable computers protected by current and supported anti-virus with centralised reporting? If not, please detail how many are not? (An estimate is sufficient)	N/A	Information Security exemption applied to response
		Do you have a policy for selecting Microsoft security updates to be applied? If so, is the policy to apply all security updates or only a subset?	N/A	Information Security exemption applied to response
		Have all Microsoft security updates described as "critical" in the past 2 years been applied within 1 month? If not, please detail how many were not applied within this time? (An estimate is sufficient)	N/A	Information Security exemption applied to response
		Have computers or servers managed by the trust been affected by malware in the last 2 years? If so, please detail the names of the malware involved (such as "Wannacry")?	Yes	Wannacry- please refer to Trust public statement on this attack,

File reference	W17FOI399
Key words	IT security
Date of release	14/09/2017
Attachments	Yes

Freedom of Information Act Disclosure log - Reply Extract

You asked us

I am writing to you under the Freedom of Information Act 2000 to request the following information from Plymouth Hospitals NHS Trust: answers to four sets of questions in the attached spreadsheet regarding the use of information technology. The italicised information in the 'Answer' and 'Details' columns gives information about the ideal format for each of the answers.

Our response

Please find the attached spreadsheet. The Trust has provided answers where we were able to do so and where the response does not compromise the integrity of our patient information systems. Where integrity is affected, the Trust has refused the request beyond that published on the Trust's website. Please refer to our legal statement as exemptions apply to the questions you have asked.

Our legal statement relating to the use of exemptions

Introduction

Section 31 and 38 apply to all of the questions you have asked where indicated by 31/38. We are sorry that we cannot be more helpful, but trust that you will understand our approach in light of the risks associated with responding, particularly in light of recent national news events about cybercrime.

We have for some time adopted a similar approach to all requests about our integrated network security and believe this is necessary in maintaining the highest levels of security.

Exemptions applied

Section 31.-(1) (a) the prevention or detection of crime applies, as does 31.-(3) neither confirming nor denying we hold the information requested.

Section 38-(1) (a) and (b) the Health and Safety exemption applies. Additionally section 38.-(2) applies in that we are neither confirming nor denying we hold the information requested.

Exemptions use rationale

This disclosure would prejudice the prevention and detection of crime and any information, albeit confirming what we hold or do not hold could assist criminals and place our patients and staff at harm. The Trust has provided a more detailed rationale below for each exemption used and applied them following the careful

consideration of submissions made to a Public Interest Test in deciding the outcome of our response to you.

Section 31 – Law enforcement- prevention of crime

We consider this exemption applies because disclosing details of our security arrangements could prejudice the security and integrity of the Trust's network and increase the risk of unauthorised access to information held by the Trust, much of which is confidential and sensitive. The level of detail that would be released would enable external parties, who are not privy to the confidential aspects of Trust's IT systems, knowledge of our security equipment and by association its integrated network security. The Trust employs a range of security tools to mitigate the risk from different types of security threats. Firewalls, Intruder Detection Devices Antivirus and other products form a mesh of security that protects the Plymouth NHS Network and data, the more of these vectors that are known, the weaker the security of the network protection. There is a real risk that this knowledge could assist external parties in attempting a cyber-attack/hack into the Plymouth NHS Network. The anticipated harm from this is a breach of data protection (failure to protect information resulting in an unauthorised disclosure), data loss, and disruption to patient care through a loss of IT services. The severity of harm is extensive with millions of patient records put at risk of unauthorised disclosure.

Section 38 Health and Safety

Such disclosures also endanger the physical or mental health and safety of patients and staff. The dangers have become self-evident from recent events reported in the news, including delays to treatment and diagnostics to name but a few. Any failure of our infrastructure endangers both the physical and mental health of our patients and exposes them to danger.

Additionally

For Q1, cell 3E of the spreadsheet Plymouth Hospitals NHS Trust is confirming in accordance with section 1 (a) of the Act that it does not hold the information requested in any collated format. There is not central list of individual systems that contain patient data nor of their functionality. We could not locate, extract and collate the requested within the limitations of the Act and be assured of its accuracy within the time limits specified in the Act. It is therefore considered exempt from supply in accordance with section 12(1) of the Act – Request exceeds the appropriate limit by virtue of section 13.-(1)(a) – The Cost of Compliance exceeds the appropriate limit.

Attachments included: Yes