

FOI 2189

22<sup>nd</sup> February 2024

## **FREEDOM OF INFORMATION ACT 2000 – INFORMATION REQUEST**

---

### **Question:**

**System type – PACS**

**Supplier name -**

**System name -**

**Date installed -**

**Contract expiration -**

**Is this contract annually renewed? - Yes/No Do you currently have plans to replace this system? - Yes/No Procurement framework - Other systems it integrates with? – Total value of contract (£) – Notes - e.g. we are currently out to tender**

### **System definitions:**

**Picture Archive and Communications System (PACS) – A picture archiving and communications system is used for diagnostic images.**

### **Response:**

**System Type – PACS**

**Supplier name – Sectra Ltd**

**System name – \***

**Date installed – Originally installed in 2019**

**Contract expiration – 10 year contract therefore 2033**

**Is this contract annually reviewed? – No**

**Do you currently have plans to replace this system? – No**

**Procurement framework - Regional contract through BSO**

**Other systems it integrates with? – \***

**Total value of contract (£)** – This information is not held by the Trust. You can submit a Freedom of Information request directly to BSO, who may hold this information, at the following email address:

[Foi.bso@hscni.net](mailto:Foi.bso@hscni.net)

## **Notes – Regional Contract**

System definitions:

Picture Archive and Communications System (PACs) – a picture archiving and communications system is used for diagnostic images.

## **\*Section 31(1)(a)(b) – Law enforcement**

### **Harm**

The provision of health & social care services in the Southern HSC Trust is information led with the recording of all service user information as well as staff information. The recording of this information is fundamental to the provision of services and the management of our health and social care services. The majority of the information we hold, is electronic with numerous information systems supporting the delivery of our services such as appointment booking, clinical systems supporting the delivery of care in theatres, laboratories, radiology, intensive care unit as well as supporting social care in children and adult service, mental health and disability.

All of this electronic data, whether held on premise or using cloud services is extremely valuable. Therefore by providing information on any information system, infrastructure or networks would be useful to cyber criminals by enabling them to determine any vulnerabilities that might exist or enable them to use targeted phishing attacks.

### **Factors favouring disclosure**

The public are entitled to know how public funds are spent and how resources are used within Health & Social Care. By providing information to the public on the information systems, network and infrastructure this would provide assurance to the public that the information they provide is being managed, stored and used in a secure way. This information could also potentially reduce costs and public sector spend by introducing more competition in the procurement of systems and infrastructure components.

### **Factors Favouring Nondisclosure**

The disclosure of this information could compromise the ability of the Trust to function with increased cyber-attacks and potential ransom attacks. Disclosure could compromise the Trusts (and wider HSC) tactics in terms of Network Security increasing the risk of a Cyber-attack.

Whilst security measures are in place, no network is completely secure and releasing information which may increase the vulnerability of the Trust's network. This increase in vulnerability will require more resources within the Cyber Security Team to manage and address any threats, thus reducing their ability to provide a proactive approach to network security.

The cumulative effect of releasing information in relation the Trust (and wider HSC) IT infrastructure and linking this with other information could potentially provide cyber criminals the opportunity to conduct a successful attack on the HSC network.

The HSC has a duty of care to the population in terms of protecting both the information it holds, but also protecting information systems which are critical to the delivery of safe and effective care. Without the availability of these system, information would not be available for life saving diagnostics, delivery of emergency care and the safeguarding of children and adults. Release of information to the word at large could compromise patient and service user safety.

### **Balancing Test**

For the public interest test, issues that favour release need to be measured against the issues that favour non-disclosure. The public interest is not what interests the public, or an individual, but what will be greater good for the community as a whole.

The Trust is responsible for the provision and management of health and social care for the population of the Southern Trust area, the security of the Trust's network and infrastructure is critical to enable the Trust to deliver services. The maintenance of services is of paramount importance to the Trust, securing highly sensitive information about its network.

The Trust must protect its network and information from any cyber threat that would impact on the operation of the services it provides. The Trust objective is to provide high quality, safe and effective care and where there is a risk to that objective the Trust is duty bound to prevent the release of information which may assist those persons who are intent on committing a cybercrime.

At this time, it would not be in the public interest to release this information. The Southern HSC Trust will not disclose information that could harm its ability to provide a critical service and compromise its ability to deliver high quality, safe and effective care to the population.

**Email:** [FOI.team@southerntrust.hscni.net](mailto:FOI.team@southerntrust.hscni.net)