NHS
West Norfolk
Clinical Commissioning Group

Freedom of Information request & West Norfolk CCG response

WN-2017-00020 – Protecting Patient Data

1. **How many of the GP practices within your CCG have switched on 'Enhanced Data Sharing' from TPP?**

   NHS North Norfolk CCG – 14 SystmOne Practices
   NHS Norwich CCG – 23 SystmOne practices
   NHS South Norfolk CCG – 18 SystmOne practices
   NHS West Norfolk CCG – 13 SystmOne practices

   All practices are enabled with Enhanced Data Sharing

2. **How is patient data being protected from being viewed by individuals who are not involved with that patient's care?**

   The SystmOne Enhanced Data Sharing model is based on consent from each unit where the patient is registered to receive care, this establishes a 'legitimate relationship' with the patient. The default in all units is not to share any information recorded at the unit out to others. If this default setting has not been changed, no other unit is able to see information recorded elsewhere. Where the patient has consented to share their information with other units in their care, their information at that unit is made 'sharable' but the receiving unit needs to record that patient has consented to that information being viewed. The sharing model uses a share out/share in process at each organisation or service where the patient is receiving care.
   If the patient is not registered for care at a unit/organisation, there is no legitimate relationship established and their information cannot be viewed by simply searching for the patient.

All access to the clinical system is controlled by the use of NHS Smart cards and all access to records is fully audited and there are alerts in place to notify Caldicott Guardians in practices of any consent override activity.

3. **How do patients with sensitive medical issues eg. Mental Health, HIV positive, early pregnancy, prevent their data being shared?**

Functionality exists within SystmOne to either dissent to sharing the record with other services, or to generally share the record but to mark specific consultations as 'private'. This means anything marked as private is only viewable to the unit adding the information, but would not be available to other units.

4. **How is the CCG working to ensure data protection compliance and the avoidance of misuse of the data?**

GP practices, as independent contractors are responsible for compliance with Information Governance regulations. The CCGs have provided information and guidance to practices to ensure they are able to meet these Information Governance requirements. The information provided includes information on fair processing models and information for patients on what sharing means to them and the choices they have in relation to this.

5.

a) **Does SystmOne have the capability to identify unauthorised access to a patient record by a user not involved with the patient's care?**

Yes, there are a number of audit reports and alerts built in to SystmOne, in addition to this, there is also functionality within the patient online system where the patient themselves can see which units they have been registered at, what consent has been recorded at those units and which individuals have access their records.

b) **If so, how is this unauthorised access to patient data reported to the CCG?**

It is a practice responsibility to perform initial investigations in to any suspected unauthorised access, if the practice feels there is no legitimate relationship between a patient and a particular unit, they can then escalate to NHS England who provide direct IG support to practices and may also contact the CCG Information Governance lead for support with managing the formal reporting via organisations Caldicott Guardian/police/ICO etc depending on the nature of the breach.

6. **How is the CCG planning to report unauthorised access to the patient?**

There have been no known breaches to confidential data to date but the practice would have that conversation with the patient, possibly supported by the CCG if required.

7. **What plans does the CCG have to handle data protection claims from patients whose data has been illegally accessed?**

There have been no known breaches to confidential data, however in the event of such, as per response to question 4. The GPs are independent contractors, the practice should follow their IG incident management procedures and conduct a full investigation and take immediate action as necessary to stop any further data being accessed. The practice would follow the NHS Digital IG Serious incident guidance, and dependent on the severity of

incident this would also be reported to the Information Commissioners Office the guidance has specific criteria such as ensuring that patients are informed when a breach has occurred and to advise the patient they have the option to make a complaint. If the CCG is made aware of such a situation the CCG would contact the practice to instigate the above process and also inform NHS England as their responsible organisation. The CCG encourages all practices to comply with fair processing requirements that inform patients about how their data is shared allowing them the option to opt out and to learn more if they wish. By following these Information Governance requirements, practices are doing everything reasonable that is within their control to safeguard patient data. In the event of a data protection claim, the practice would provide the evidence of their fair processing model to the ICO along with a full investigation into the incident.