Balancing Commissioning needs with Data Privacy

World Class Commissioning is driving the creation of new databases of patient level data

The repurposing of clinical data for Commissioning, Performance Management, Service Level Agreement Management (SLAM) and other Secondary Uses is key to improving health outcomes. The NHS Spine/Secondary Uses Service (SUS) is currently the primary source of this data. However, there is a need for more detailed locally-held data to support Secondary Uses.

Most NHS organisations maintain a variety of Patient Identifiable Data (PID) collections to support these functions in formats ranging from sophisticated data warehouses to simple spreadsheets. Unfortunately, most repurposing of PID run counter to *Confidentiality: NHS Code of Practice* and the *Care Record Guarantee (CRG)* and reflect the widespread lack of awareness of the required handling of Patient Identifiable Data.

Information Governance requirements forbid the use of Patient Identifiable Data for Commissioning

The *Health and Social Care Act 2001 (HSCA)* states that, except under certain circumstances, "patient data must only be used in a non-identifiable form". These privacy requirements extend beyond SUS to PID that resides and is used external to SUS: in particular, locally-held data.

Confidentiality defines policy guidelines on the collection, storage and management of patient data. Clinical data being repurposed for secondary uses must be provided in de-identified form by default. In the instances where there is a need to link across different data sets or over time, pseudonymised data should be used.

The implementation of *Confidentiality* and the CRG will require changes in working practices wherever Secondary Use data is needed. Accordingly, the expectation is that NHS organisations should have or be implementing systems and processes to restrict the use and disclosure of Patient Identifiable Data to those activities that are directly concerned with or support patient healthcare.

These legal and policy requirements have been in place for years now. Under Section 60 of the *HSCA*, the *Patient Information Advisory Group (PIAG)* has given extensions on compliance due to a lack of a comprehensive solution. But time is running out. Repurposed clinical data must be pseudonymised by "P-Day" April 2009.

SAPIOR
ENABLING ETHICAL DATA SHARING

Are you complying with Data Privacy laws and policy?

Despite being producers of Patient Identifiable Data, Clinicians, PCTs, MHTs, Acute Trusts and other Data Providers are legally required to refrain from using PID for purposes other than direct healthcare. At present, many users seem either unaware of the details of the policy or choose to ignore it.

According to the *Care Record Development Board Working Group*, mechanisms to enforce Confidentiality guidelines are not in place, resulting in a gap between policy and practice. Many Data Providers are gaining access to clear data for purposes they feel are legitimate and generally there is no comeback for breaching the policy unless an egregious breach has occurred.

> *Despite the use of role-based access controls and password systems to control data access at the local level, the attitude of many users towards the sharing of identifiable data is that access should be allowed where it is required for users to "do their job". This is in part because it is very difficult to perform certain tasks without access to clear data (e.g. record linkage); and because users feel their professional ethical codes allow them access to data if it is "in the patients' best interests".*
> *Care Record Development Board Working Group Report on the Secondary Uses of Patient Information*

Consequently, most NHS organisations are directly breaching privacy laws and DH guidance and are putting themselves at risk of highly damaging privacy breaches.

De-Identify repurposed clinical data and let your Information Governors sleep at night

Until you are aware of all of the instances in your organisation where PID is repurposed for secondary uses – and where that data is held, it will be impossible to assess and control your exposure.

- Make an inventory of all the instances where Patient Identifiable Data is being used and for what purposes.
- Make a clear distinction between occasions where individuals act as data providers (and produce clear data) and where they act as secondary users (and have no automatic right to see clear data) in order to prevent the inappropriate disclosure of PID.
- De-identify all repurposed clinical data by default.

Sapior has been de-identifying all Spine/SUS data since 2004 and is the defacto standard. Our innovative Data Privacy Compliance solutions are easy to build into your existing infrastructure. Call us so we can help you get some sleep.

Sapior Ltd
16 Byron Avenue
London
E18 2HQ

T: +44 (0)20 7060 2965
F: +44 (0)20 7748 0970

www.sapior.com

SAPIOR
ENABLING ETHICAL DATA SHARING