PARiP is the easiest way to protect both patients and staff

Does your organisation de-identify patient data whenever it is re-purposed for non-clinical work or even for mobile working? The easiest way to enforce policy and ensure privacy is to automate the pseudonymisation of clinical data before it's re-purposed.

PARiP can be applied incrementally by application or comprehensively across the organisation using a data warehouse without affecting the use of patient identifiable data for the original clinical purpose.

PARiP= Pseudonymise All, Re-identify if Permitted

PARiP reduces the opportunity and ability for accidental and malicious privacy breaches to occur. With PARiP, once data is de-identified, vital analysis can take place without threatening the confidentiality of personal information.

If analysis identifies individuals who would benefit from further medical intervention, the reversibility of pseudonymisation allows re-identification to be done in a controlled manner. In fact, re-identification should ideally be executed by the patient's GP.

When your next **data breach** happens, make sure you're **not caught out**.

Sapior is a British company with an extensive background in data management and business intelligence. We understand the value of using data for a host of activities. But we also recognise the vital importance of fostering trust and confidence in the people whose data is being used. It is our mission to enable ethical data sharing.

Used by SUS, Sapior provides the de facto national standard for pseudonymisation. The Sapior module employs patent-pending multi-stage technology ensuring that the solution is highly scalable in all aspects. But it is presented in an easy-to-use solution for local organisations with limited IT capabilities.

It may be some time yet before local NHS organisations are spot checked by the Information Commissioner's Office. In the face of a data breach, how will NHS organisations justify using local data in an identifiable format, if privacy-enhanced pseudonymised national data can be used for the same or similar purposes?

Learn how we can help you protect your patients and staff by minimising the impact of an inevitable data breach.

SAPIOR
ENABLING ETHICAL DATA SHARING

020 7060 2965 or info@sapior.com
www.sapior.com

Concerned about the **privacy** of **patient data**?

Despite the abundance of recent data security failures, we can expect incidences of privacy breaches to rise. This is due to the simple fact that the more data is used, the greater the risk of a privacy breach.

Security experts agree some breaches are inevitable. With the human factor being the weakest link, perhaps the current state of security is as good as it can get. Regardless, what is needed is a greater focus on ensuring privacy despite a breach. In this way, with any breach, the privacy of the data itself is protected as much as possible and staff are protected against accidental data handling errors.

The public sector is only now coming to realise that ensuring privacy, which is not yet fully addressed by security, is key to guaranteeing trust and confidence. The importance of privacy and confidentiality has been one of the key tenets of the medical profession for centuries. What is changing for healthcare organisations is the increasing use of patient data for commissioning, performance management, and many more "secondary uses".

The **more** data is **used**, the **greater** the **risk** of a privacy breach.

SAPIOR
ENABLING ETHICAL DATA SHARING

The use of patient data is **on the rise**

According to the DH Public Health Information Strategy, "putting information at the centre of health" is vital to both quality of care and efficiency of operation.

So far as medical practice is concerned, the availability of more detailed information and the use of more sophisticated techniques open up possibilities for more penetrating analysis which will pay off in improved clinical outcomes.

NHS organisations must re-purpose patient data for a wide spectrum of secondary uses including:

- Commissioning
- Service Planning
- Performance Management
- Clinical Audit
- Research
- Public health
- Public enquiries

For the developing commercial environment of "world class commissioning", clinical data is vital to determine cost effectiveness of health provision. The analysis of need and service provision within a geographical area is fundamental to the business cases that Monitor expects to evaluate in authorising and subsequently checking performance of Foundation Trusts.

Along with these examples of recent initiatives, the Prime Minister's recent call for a "personal" and "empowered" service highlights the dilemma between using patient data and ensuring its privacy.

"Personalisation"—especially where it requires tracking of individuals over time to judge the cumulative effect of health interventions—demands a robust approach to handling data. Similarly, "empowerment" demands that stakeholders or actors in the health sector need to be able to access and analyse data to help them improve service, without endangering the ethical values of patient confidentiality.

As discussion between professionals on all aspects of medical practice has increasingly emphasised the need for "evidence-based" approaches, an increasing load has been placed upon the collection and analysis of clinical data.

So the dilemma intensifies. And the need to protect the privacy of patient data itself becomes more acute.

> **"Where there is a need to link data from different data sets or over time, linked pseudonymised data should be used..."**
>
> *Report of the Care Record Development Board on the Secondary Uses of Patient Information, p11, section 4.2.i*

Mind the gap: **De-identify**

The law and DH policy require NHS organisations to de-identify patient data that is re-purposed for secondary uses.

By April 2009, NHS organisations should be using the Secondary Uses Service (SUS) for performance monitoring, reconciliation and payments following *The Operating Framework for 2008/09 (p35, section 3.35)*.

Pseudonymisation day or "P-day" is the beginning of the movement to enforce *Confidentiality: NHS Code of Practice*, ensuring that all re-purposed data is provided in de-identified form.

SUS promises to be a tremendous resource for cross-region comparison. Patient data is pseudonymised and re-identification is available only on a permission-basis. Comprehensive pseudonymisation ensures that if all else fails, the data itself is still protected to a reasonable degree. Without it, patient data is only protected with the strength of the weakest link in the chain of security measures.

But SUS is only a partial solution. There is a much larger body of detailed locally-held data that can never be protected by SUS.

> **"It is not justified to share information that identifies people, when anonymised or statistical information could be used as an alternative."**
>
> *Information Commissioner's Office (ICO) Framework Code of Practice for Sharing Personal Information, p8*

Ever-changing, locally-held data requires a local pseudonymisation solution to ensure both patients and staff are protected against privacy breaches.

Until recently, Fair Processing Notices have been used to justify the re-purposing of clinical data. But this is being reviewed by the ICO and organisations are now expected to use de-identified data wherever possible.

Though DH provides guidance, Information Governance (IG) responsibilities have been locally devolved. And the requirement to enforce IG standards through local disciplinary measures is on the rise.

What are you doing to uphold policy and protect patients and staff from privacy breaches?

> **"At present, many users seem either unaware of the details of the policy or choose to ignore it, and mechanisms to enforce the Confidentiality guidelines are not in place.**
>
> **This has the result that there is a gap between policy and practice.**
>
> **Secondary data users 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."**
>
> *Secondary Uses Service Pseudonymisation Impact Assessment Study, p9, section 2.2.6*