Sapior De-identification:

Pseudonymisation Functionality all wrapped up in a box

> ***"Pseudonymisation functionality will have to be implemented by local organisations to support the use of pseudonymised data for secondary purposes"***
> ***Pseudonymisation Implementation Project Local NHS Data Usage and Governance Planning Template***

The Department of Health (DH) lists the following pseudonymisation functionality alternatives for local NHS organisation:

- building it in-house
- extending local supplier systems one by one
- commissioning an external service or
- implementing a specialised "black box".

Of course, each has its own set of pros and cons. But consider this key point...

Pseudonymisation is Middleware

Embedded between your data sources and end user applications, **it will be completely relied upon and so must be completely reliable**.

Sapior's De-identification Appliance provides the most robust standard of pseudonymisation functionality to meet DH Pseudonymisation Implementation Project (PIP) requirements in an easy-to-manage, web-enabled black box.

Sapior De-identification provides the reliability and peace of mind expected from off-the-shelf middleware, without the ongoing headache and cost of an in-house solution.

Meets your timescales
Mature and proven, Sapior De-identification meets PIP technical requirements in a timely fashion so you can focus on business process changes and other PIP requirements. Not to mention concentrating on providing excellent healthcare.

Adapts to local needs
Another data source? New end user application? The Sapior appliance is designed to meet general data management requirements, is accessible by all end user applications and can easily be customised to adapt to your changing environment.

Adheres to changing standards
The Information Standards Board for Health and Social Care (ISB) and the International Organization for Standardization (ISO) are both currently developing standards for pseudonymisation. Sapior De-identification accommodates changes in relevant technical standards with minimal effect on your technical team and business processes.

"I am pleased to be able to tell you that your application for Section 251 support has been provisionally approved for the purpose of the pseudonymisation activity, and that Members noted the use of technology in the pseudonymisation process to be highly commendable."
Patient Information Advisory Group (now NIGB-ECC) comments on Sapior technology

Sapior De-identification is an intranet hardware appliance that resides in a local data centre. It is configured via a browser and speaks the industry-standard XML protocol (SOAP).

Sapior De-identification provides all of the PIP pseudonymisation functionality requirements and more.

Sapior **de-identifies** Patient Identifiable Data (PID) by replacing it with pseudonyms or unique identifiers. This is done on a consistent basis so that patient records are distinguishable and linkable, but not identifiable. Different pseudonym sets can be created for different departments and organisations.

Sapior **re-identifies** or rolls back to PID on a case-by-case permission basis to authorised NHS staff. The automated re-identification process eliminates manual, resource-dependent and time-consuming encryption key management.

New Safe Haven requirements (PIP-R9)
Implementing restrictions on identifiable data access can be achieved in two ways. Pseudonymised data can be supplied by default and specific records can be re-identified for authorised staff with the required logs and audit trails. Alternatively, both sensitive information and pseudonyms can be stored in the database and access controls used to uphold appropriate access. However this will put significant strain on the access control environment.

Access control functionality (PIP-R10)
Sapior plugs directly into the local access control environment.

Pseudonym formatting (PIP-R12)
The Sapior appliance provides shaped pseudonyms that meet the technical formatting requirements of local applications.

Logging/Auditing (PIP-R14)
Sapior's re-identification feature provides logging and auditing for access to identifiable data. The automated process eliminates the security risks and resource requirements commonly associated with key management.

Additional features

- Hardened appliance minimises security risks
- Backup/recovery
- System availability monitoring (optional extra)

Sapior De-identification fits within the Extract/Transform/Load (ETL) process, after cleansing, and before the database load. Sapior is called in two instances: initially, when loading the database, and later, in the mart loading or report generation process.

What you need is what you get

Consistent error-free pseudonymisation – Avoids the nightmare of reloading your database and purging all dependent reports.

Maintain history – Accommodates temporary NHS numbers and other slowly changing sensitive values

Stay clear of ETL – "Black box" integrates with different platforms, scales on demand and is robust to power outage or disk failures.

Secure machinery – Security-hardened appliance provides multiple levels of security including arbitrary pseudonym assignment. "Two key" data store protects stored sensitive values, pseudonyms and encryption keys. "Agile" encryption adapts to developing encryption technology.

Meet developing needs – Accessible and easily customisable to your evolving application environment.

Keep abreast of standards – Adheres to changes in pseudonymisation, encryption and other relevant technical standards

Ear to the ground – Our specialists keep your solution up-to-date with industry

SAPIOR
ENABLING ETHICAL DATA SHARING

Sapior Ltd.
16 Byron Avenue
London E18 2HQ

T: 0870 423 2580
F: 020 7748 0970
www.sapior.com