Losing sleep over privacy risks?

De-Identify your data first. It reduces privacy breach risks, minimally impact users and the ICO expects it.

The ICO expects you to minimise your use of PII
It's quite simple. The more you use Personally Identifiable Information (PII), the more you risk a privacy breach. In accordance with the Data Protection Act 1998 (DPA), the Information Commissioner's Office (ICO) expects organisations to minimise their use of PII whenever possible and, of course, to keep it secure at all times.

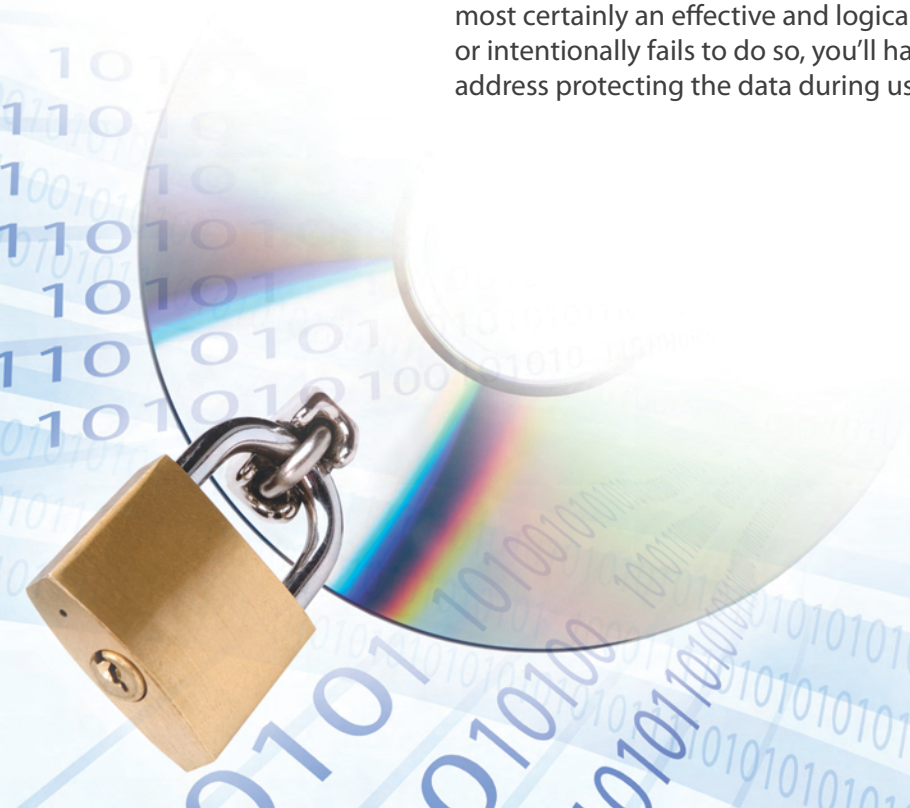
> *"We expect organisations to adopt a privacy-friendly approach, e.g. avoiding or minimising the use of information in a form that identifies people."*
> Sharing Personal Information: Our Approach, ICO

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

De-Identified data is more private
Most organisations believe they are already upholding "need to know" policies but that their workers "need" to see and work with Personally Identifiable Information. However, a middle ground does exist between PII and data that has been protected by encryption and thus unusable until decrypted.

Data that has been De-identified can still be used to analyse patterns and distinguish the activity of specific individuals without exposing the underlying people. Unlike identifiable data, distinguishable data protects personal identities. In addition, compared to encrypted data, distinguishable data minimally impacts data users.

Automatically enforces "need to know" policies
If you rely on people and processes to uphold your privacy policies, there will always be an opportunity to circumvent them. Encrypting data for transport or storage is most certainly an effective and logical way to protect it. However, if someone forgets or intentionally fails to do so, you'll have a potential breach. And this doesn't even address protecting the data during use.



SAPIOR
ENABLING ETHICAL DATA SHARING

By de-identifying your data from the start, you can automatically enforce "need to know" policies. Rather than holding Personally Identifiable Information and trying to limit its use to the few users with permission, make data available in a de-identified format and then give access to PII only on a case by case basis.

Health Information workers use it
Health data is confidential and subject to the Health and Social Care Act 2001 (HSCA), in addition to the DPA. The NHS Spine/Secondary Uses Service (SUS) was set up in part to ensure that the HSCA and the NHS *Care Record Guarantee* and *Confidentiality: NHS Code of Practice* are automatically enforced across a multitude of NHS organisations and users.

The *SUS Pseudonymisation Impact Assessment Study* found that most processing produces the same results when using Personally Identifiable Information or de-identified data. Also, business processes that didn't require PII – but were using PII because that was how the data was supplied – would be unaffected by using de-identified data.

In the instances where PII was necessary, many of these processes could be adapt to using de-identified data if various technical considerations were met. Alternatively, data could be re-identifed in the final stages of work for a limited data set rather than starting work with an entire set of PII.

De-identify first and let your Information Governors sleep at night
De-identifying your data is the first thing you should to. You can re-identify it later when it is necessary. The rest of the time data is being used, Personally Identifiable Information will be safe away from curious or even malicious eyes. You will reduce your use of PII and improve its protection during use.

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.

There really is no excuse to use Personally Identifiable Information when De-identification is possible. 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