



# Safeguard patient data through de-identification, encryption, and in-workflow re-identification

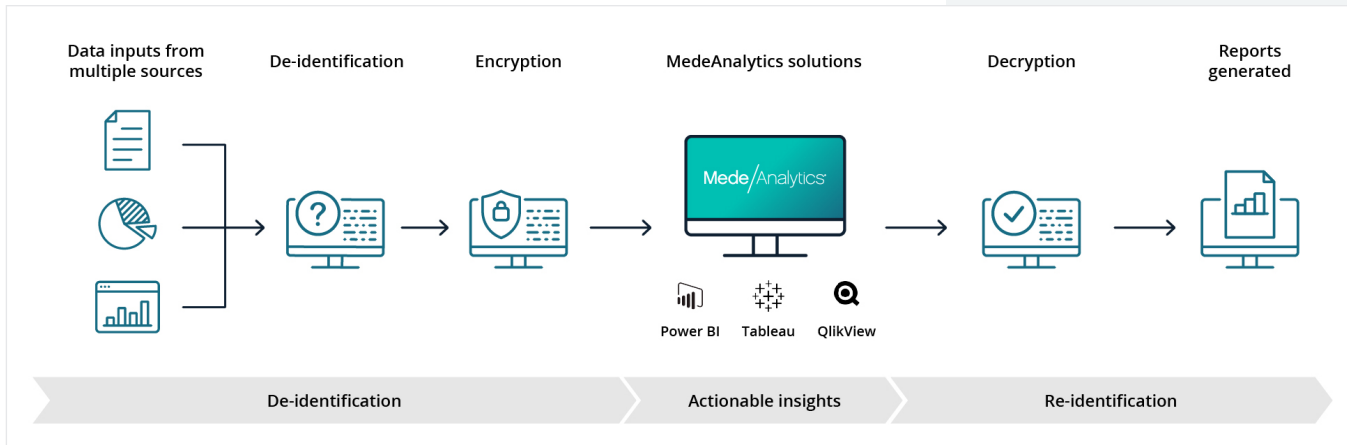
With 1.5 million patient interactions taking place every day, the NHS has an incredible wealth of data that's growing at a rapid pace. That data is vital to organisations for continuing to improve care planning and drive more optimal outcomes. However, this expansion in the use of data comes with growing risk. A 2021 survey showed that over 81% of UK healthcare organisations suffered some form of data breach or attack with 38% of them having financial repercussions.

To ensure this data remains private and secure, NHS organisations are required to remove personal identifiers from data sets prior to use for any purpose other than that of direct care. Not properly securing this information contributes to the majority of the reported data breaches by the Information Commissioner's Office, resulting in large fines and reputational damage for NHS organisations.

The MedeAnalytics Privacy Framework is a comprehensive mechanism designed to pseudonymise information at the source, removing the ability to identify any patient or service user and be used in a safe and secure manner.

## Why you need the Privacy Framework

As more data is being shared at increased frequency across health and care systems, it has never been more important to ensure that only the appropriate data is accessed at the right place, at the right time, and by the right personnel. The MedeAnalytics Privacy Framework allows information to be securely shared using state-of-the-art encryption as well as pseudonymisation in a stand-alone, end-to-end product agnostic solution.



## With MedeAnalytics Privacy Framework, you can:

- Pseudonymise identifiable data row by row at a data item-level in its source system
- Pseudonymise in real-time
- Allow real-time, re-identification for appropriate users within workflow
- Encrypt data as well as pseudonymise
- Have a stand-alone, end-to-end product agnostic solution
- Use a standard API to support re-identification workflows



Comply  
with data  
legislation



Provide  
pseudonymisation  
in real-time



Lower risk of data  
breaches leading to  
financial penalties



Enable only  
authorised personnel  
to re-identify data

## Benefits of MedeAnalytics Privacy Framework

- With nearly two decades of delivering solutions to the NHS, MedeAnalytics has the experience and expertise to implement privacy solutions required by the NHS. Safeguard your data, whilst also enabling NHS organisations to use the data to develop actionable insights, providing operational efficiency and better patient outcomes.
- The Privacy Framework extracts identifiable patient data, de-identifies the information, and uses public key encryption, also known as asymmetric encryption. Our encryption process works across all relevant datasets, including primary and secondary care as well as public health, social care and community services.
- The resulting anonymised data sets are securely transmitted to the MedeAnalytics solution, where they are linked with existing data sets without the need to re-identify the data to perform the linkage.
- MedeAnalytics can receive and process data from a single source or multiple sources as well as connect data to third-party visualisation tools such as Power BI, Qlikview, Tableau and more.
- Patient data can be re-identified by specific users who have the appropriate legal permissions. Re-identification uses a separate single-use private key, which is managed by a third-party to help ensure privacy.
- Re-identification is supported by strong authentication and ongoing auditing. The re-identification takes place in the client's web browser and can't be downloaded.
- To ensure data security, MedeAnalytics has access only to the pseudonymised data, but not the private key. The "trusted third-party" has access only to the private key, not the patient data.



Learn more about MedeAnalytics at  
[www.MedeAnalytics.co.uk](http://www.MedeAnalytics.co.uk)