PRIVACY ANALYTICS
a QuintilesIMS company

ACADEMIC MEDICAL CENTERS

Academic Medical Centers

The digitization of healthcare has led to an explosion in the volume of health information. Turning this vast trove of patient data into knowledge requires it to be accessible for research and other secondary purposes. De-identification removes the protected health information (PHI) from patient data in order to safeguard privacy. To be useful, however, it also needs to preserve data quality. It's why responsible data sharing begins with risk-based data de-identification.

Rich Data for Research

The ability to look at entire populations of patients for trends and patterns in the data is enriching our understanding of the causes, patterns and progression of diseases and opening up new pathways in prevention and treatment based on evidence.

Increasingly, registry data is being linked to other sources of patient information, creating more comprehensive offerings with rich, detailed information about each patient. It is enhancing the analytic value of these datasets and driving huge demand for them.

De-identifying Data

Data de-identification safeguards patient privacy by removing protected health information (PHI) from the data. The use of a risk-based de-identification means that the risk of a person being re-identified from their data is measured and managed. It allows data quality to be maximized by retaining the nuance and granularity needed for research.

Use of a risk-based approach to de-identify data, like HIPAA's Expert Determination method, is recommended by the world's leading privacy organizations when anonymizing patient data for secondary use. It is an approach that not only avoids the problem of consent bias but provides data owners with flexibility in responding to multiple, unique research requests.

The Experts

Privacy Analytics is the only company that uses a scientific, risk-based method to de-identify data for healthcare. Our approach is consistent with HIPAA's Expert Determinations method and follows the recommendations and guidelines of the EU General Data Protection Regulation, HITRUST Alliance, the Institute of Medicine, PhUSE, and the Council of Canadian Academies.

Privacy Analytics' software solutions help protect organizations against re-identification risks by implementing a consistent, repeatable and scalable solution to automate data de-identification for a wide variety of data formats and types.

Privacy Analytics: The only proven, responsible way to unlock the value of health data.

For more information on how Privacy Analytics can help your organization establish best practices to de-identify data for Registries see our white paper Strengthening Secondary Use

251 Laurier Avenue W, Suite 200
Ottawa, Ontario, Canada K1P 5J6
Phone: +1.613.369.4313
sales@privacy-analytics.com