eInfoGuard®

Data De-Identification Solution

BayaTree

Safeguards Protected Health Information (PHI)

BayaTree eInfoGuard is a data de-identification tool which safeguards Protected Health Information (PHI). Our revolutionary solution provides an efficient, cost effective, and flexible method for individually masking each data field - offering the highest level of security while maintaining operational usability. BayaTree eInfoGuard assists Covered Entities and their Business Associates maintain regulatory compliance.

Overview

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), eighteen (18) identifiers classified as Protected Health Information (PHI) must be secured and treated with special care. This regulation applies to all Covered Entities, organizations involved in the course of providing and paying for healthcare, and their Business Associates. Failure to comply with HIPAA can result in civil and criminal penalties.

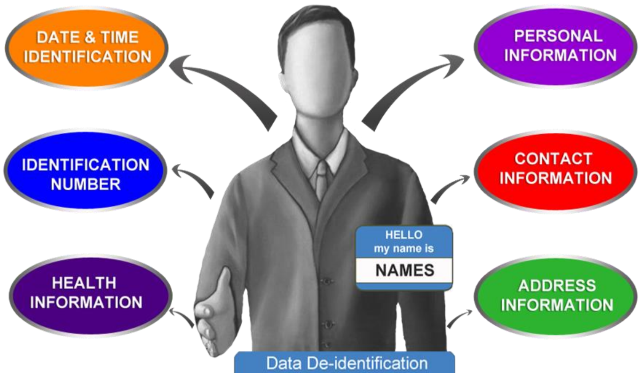
Why BayaTree eInfoGuard?

Covered Entities are increasingly asked to share data they generate in their normal course of providing services or conducting research. However, this data may contain information about patients or study participants, and sharing this could breach HIPAA confidentiality regulations. BayaTree eInfoGuard creates separate HIPAA-compliant repositories of de-identified data to support the needs of clinicians, researchers, and IT Departments.

Method

BayaTree eInfoGuard uses the Safe Harbor method for de-identification as specified in Section 164.514(a) of the HIPAA Privacy Rule. Multiple de-identification techniques are utilized:

- Random and Static Value Substitution
- Static Value Append
- Character and Positions Replacement
- Vowel(s) Substitution
- Random Shuffling
- Range Randomization
- Date Randomization
- Conditional De-Identification
- Single and Multiple Row Replacement



Solution Highlights

- ✓ Compliance and Risk Mitigation
- ✓ User-Friendly and Flexible
- ✓ Various De-Identification Techniques
- ✓ Multiple DB Support (SQL Server, Oracle, Sybase, and MySQL)

Data De-Identification Process

Identify

Sensitive data elements in various data sources should be identified. The goal of this exercise is to create a comprehensive list and description of data elements to be de-identified, and identify the associated database tables, columns, and relationships across enterprise datasets. Data elements in addition to PHI may be included.

Review

Analyze and select the data de-identification rules and techniques to be applied to the identified list of sensitive data elements and their values. This is a very important part of the process. Incomplete analysis may lead to the masking of unnecessary information or failure to de-identify when required.

Configure

This step involves the configuration of various de-identification rules, techniques, and algorithms for the identified list of sensitive data elements.

Operate

Run the configured eInfoGuard de-identification engine against the identified data sources to create a de-identified dataset.

Validate

Ensure that the de-identified data conforms to rules established in the Configure step.

For More Details, Click Here Web Site: www.bayatree.com Phone: +1-801-386-5075