Policy Driven
Dataflows

Empowering dataflows of the modern enterprise

### The Workhorse of the Modern Enterprise

The widespread use of dataflows throughout the modern enterprise is the backbone of many data-driven business models. Modern dataflows capture event data from various sources and provide it to business functions across multiple data domains. As data flows through various domains, different applications (workloads) operate on and transform the data. Since data often contains confidential and private information, there is an urgent need to gain auditability, visibility and trackability of applications accessing the data. Each data domain and/or the overall organization may wish to impose their governance and compliance policies on the data.

SafeLiShare uses recent advances in confidential computing technology to provide Policy Driven Access to Applications and Data (PDAAD) throughout a workflow, i.e., to every workload in the dataflow. Support for audit and verification functionality is now possible with SafeLiShare's PDAAD technology.

Data in modern enterprises is often decentralized and exists in multiple data domains. Many applications across the enterprise may need access to this data. Managing and granting access to these applications becomes the responsibility of the various data domains. PDAAD gives explicit recognition to data and application ownership. Data may only become accessible to authorized applications and such authorizations are granted by the data owners. At the same time, PDAAD ensures that application owners permit their applications to process specific datasets. Such symmetric authorizations are at the heart of PDAAD.

Take the use of workloads comprising an existing dataflow in a healthcare enterprise. Given the presence of sensitive and confidential data in input data sources, there is a need for auditability, visibility and trackability whenever data is made accessible to any application in a workload. PDAAD provides these capabilities to the data owners whose data is used in the workloads. Additionally, it allows application owners to authorize alternative workloads to be constructed in a pre-existing dataflow using new applications.
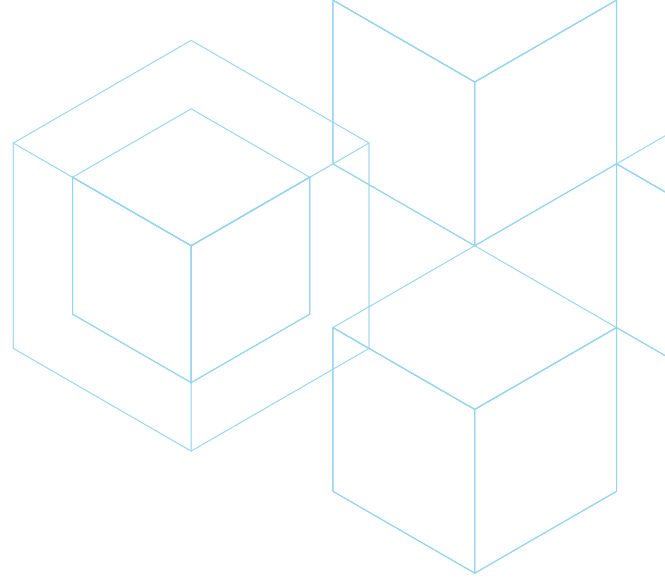
For example, it is well-known that several de-identification procedures are known to practitioners. Allowing a partner enterprise or business function to contribute a new de-identification procedure and allow it to be used to create a customized curated dataset based on pre-existing dataflows offers new revenue opportunities. PDAAD supports such new business opportunities by ensuring auditability, trackability and visibility is not sacrificed when the new procedure is invoked in a workload.

Curated Dataset

De-Identification

Normalization → De-Identification → Aggregation

De-Identification

Custom Curated Dataset
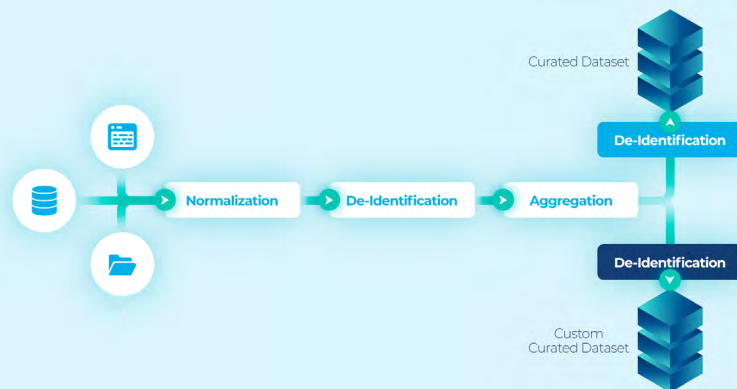
When healthcare datasets are provided for R&D purposes, HIPAA regulations require that applications processing the datasets be tracked for auditability purposes. With the use of PDAAD technology, compliance and governance rules and requirements can be fulfilled.

| Guarantee data privacy of PHI while preserving/increasing data utility. | Fulfill mandatory regulatory compliance (HIPAA, GDPR, etc.) standards. | Create and enforces new usage-based policies for data. | Enable new business models and revenue streams for all data. |

About SafeLiShare

In an era when data has become the product for many enterprises, and faces increased scrutiny due to tightening global regulations, SafeLiShare was founded with a vision to provide application specific access to data. All operations on data by applications are made visible, auditable, and trackable. Multiple governance policies can be enforced simultaneously. Powered by confidential computing technology, policies drive compliance and governance throughout an enterprises' multiple business functions, data domains, and even across to external business partners engendering a new class of business models based on ownership of data and applications.

SafeLiShare