Karlsgate

Ensuring Patient Privacy

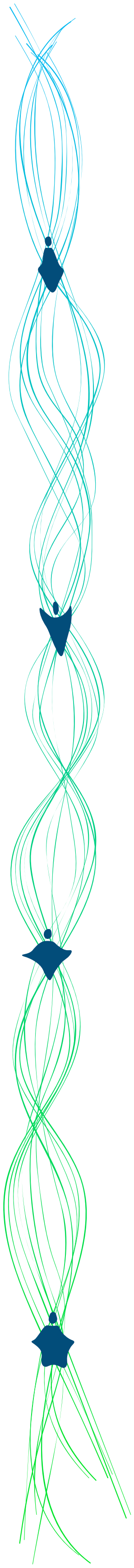
Demystifying the Power of Cryptoidentities for Secure Data Connectivity

Data sharing without exposing patient identity

Individual privacy protection and data security are issues that should keep you up at night. The healthcare industry has been sharing, posting and transmitting data for decades with little regard for disclosure risks as long as they are HIPAA compliant and have business associate agreements (BAAs) in place. Lack of public awareness and focused legislative agendas threaten to impede progress toward more beneficial applications for managing, connecting and integrating real-world data (RWD).

A new data-sharing approach is needed. The primary design consideration for this new approach must be balancing the needs for protecting individual privacy with the needs for linkage and connectivity of healthcare data. Personal data rights are a rapidly expanding field with ethical, legal, and strategic implications. For technology to keep pace with these dynamics, new mechanisms need to be designed, developed, and implemented to support a new social contract of personal data protection.

Karlsgate created Cryptoidentity™ to protect individual privacy while enabling efficient linkage of data between business associates.



What's inside:

- Understanding the true cost of trust
- Recognizing the limitations of current data-sharing methods
- Cryptoidentity: A new mechanism for a new era
- The future of sharing identifiable, real-world data
- A re-imagined privacy framework
- Protection empowers freedom to share data

Understanding the true cost of trust

Current modes of sharing identifiable, individual-level data require transferring Personal Data identifiers, like a name, address, birthday, or social security number between two business associates to match data sets. These data-sharing arrangements rely on trust that each organization will treat Personal Data securely and with integrity. A legal contract (BAA) and trust are not sufficient to truly protect individual privacy.

Patient privacy protection is lost

Whether using clear text IDs or hashed IDs, sharing data like this represents personal information disclosure and promotes the discovery of individuals. Data owners lack control over what happens to Personal Data after transferring it to a business associate. Once Personal Data is copied, it can be copied perpetually. Not only that, once information is copied, it can be used as a persistent identifier that can link activity back to a single person forever.

Data security lapses are costly

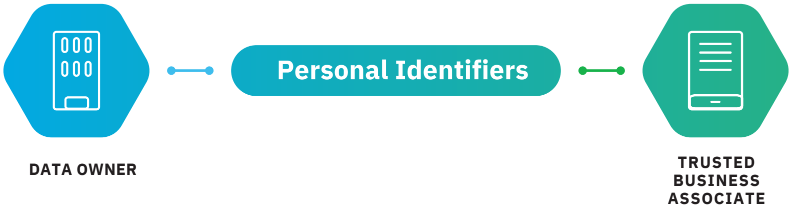
Data owners, whether they are life-sciences firms, healthcare providers, or data aggregators, are all under ethical and regulatory obligation to protect individual privacy and data entrusted to them.

- **Financial impact –** $4.45 million average cost per data breach in 2023 (1)
- **Healthcare breaches –** 527 healthcare breaches reported to HHS in 2023 (2)
- **Patient privacy –** 51.9 million patient records compromised in 2022 (3)
- **HIPAA fines –** 70% decrease in total HIPAA fines when organizations have zero-trust architecture in place (4)

Recognizing the limitations of current data-sharing methods

Name, address, birthday, social security number, and medical record numbers are a few of the common identifiers used to link and connect data sets shared between business associates. Unfortunately, though these are among the 18 identifiers of Protected Health Information, when two business associates create a BAA, they are able to send these and any other identifying information to each other as long as they have a business need and have the BAA in place. When they share the data, the three most widely-used methods for sharing these IDs for matching - Clear Text, Encryption, and Hashing - are open to significant consumer privacy and data control risks.

1. Clear IDs transmitted to a trusted business associate



Characteristics

- Human-readable identifier used for matching purposes
- Business associates gain full exposure to all identifiers
- One party lacks all control over the mapping rules and security of the data transmitted
- Trust is needed, since identifying data can be leaked

Effects On Privacy

✗ Full disclosure of Personal Data

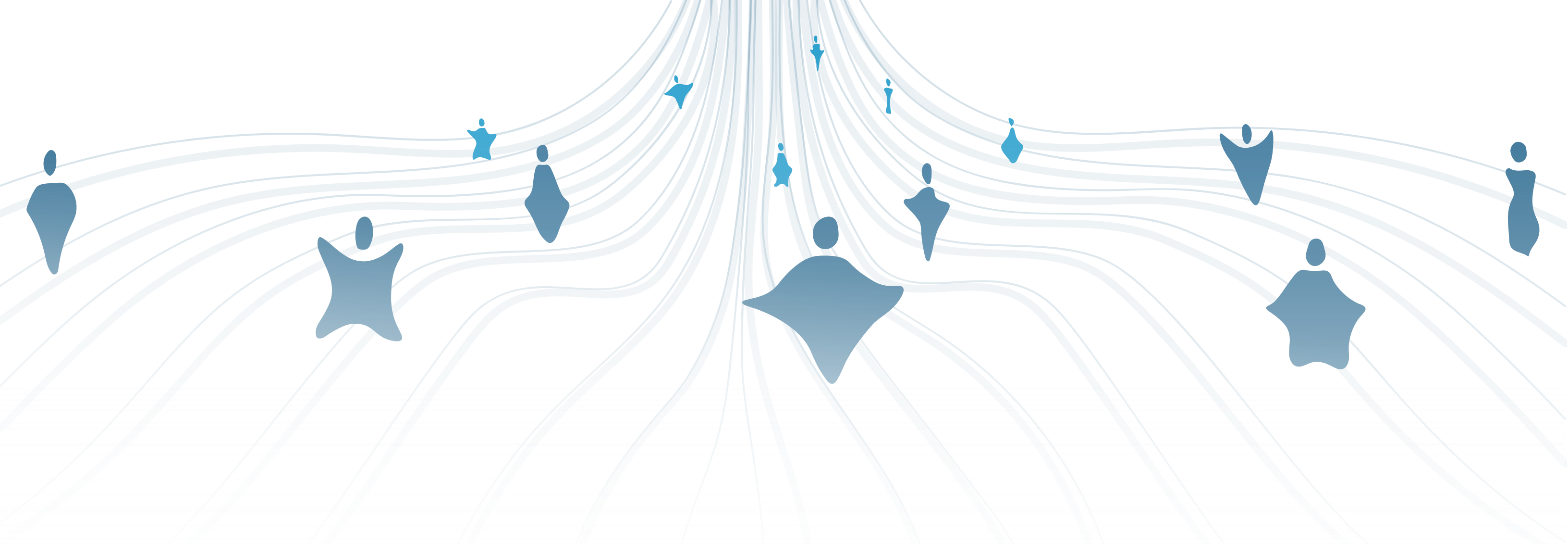
✗ Explicit consent required to transfer Personal Data in some jurisdictions

✗ A data breach at either party during transit (i.e. MoveIT) risks direct exposure to personal data

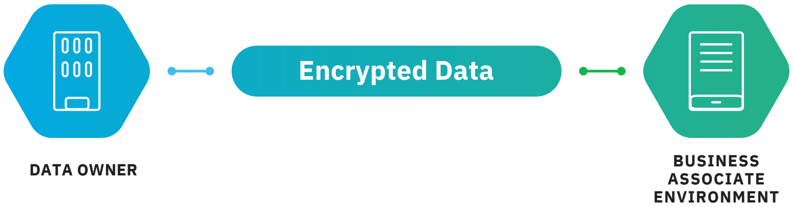
✗ Inequitable control over mapping process between sender and receiver

Security Matrix

Personal data	To the data trading partner
Are unknown identities exposed?	Yes. The entire audience is transmitted.
Can identities be re-identified?	Yes. Personal Data is openly shared.



2. Encrypted Data transmitted to business associate environment



Characteristics

- Identifiers obfuscated during transit but is decrypted back to clear text in business associate environment
- Business associates gain access full exposure to all identifiers
- One party lacks all control over the mapping rules and security of the data transmitted
- Trust is needed, since identifying data can be leaked

Effects On Privacy

✓ Underlying identifiers are obfuscated during transit

✗ Full disclosure of Personal Data when shared key is used to decrypt the data

✗ Re-identification risk to all identities since hashed identifiers can be mapped to external databases

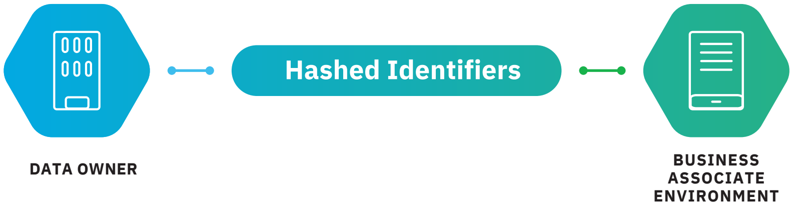
✗ Hashes serve as pseudonymous identifiers and may be classified as personal data transfers

✗ Inequitable control over mapping process between sender and receiver

Security Matrix

Personal data	To the data trading partner
Are unknown identities exposed?	Yes. The entire data set is transmitted.
Can identities be re-identified?	Yes. Personal Data is openly shared.

3. Hashed IDs transmitted to business associate environment



Characteristics

- Persistent and reusable hashed identifier used for matching purposes
- Business associates gain access to all hashed identifiers
- One party lacks all control over the mapping rules and security of the data transmitted
- Trust is needed, since identifying data can be leaked

Effects On Privacy

✓ Underlying identifiers are obfuscated

✗ Re-identification risk to all identities since hashed identifiers can be mapped to external databases

✗ Hashes serve as pseudonymous identifiers and may be classified as personal data transfers

✗ Inequitable control over mapping process between sender and receiver

Security Matrix

Personal data	To the data trading partner
Are unknown identities exposed?	Yes. The entire data set is transmitted.
Can identities be re-identified?	Yes. Stable hash values can be accumulated for later matching.

Cryptoidentity: A new mechanism for a new era

Karlsgate developed Cryptoidentity to address the current weaknesses in data sharing. This patent-pending technology significantly increases the privacy protection of identifying information over current methodologies of sharing data.

Using Cryptoidentity, identities in one data set can be linked or “mapped” to the matching identities within another data set without exposing Personal Data. Cryptoidentity operates on any two data sets that contain a common unique identifier including name, address, birthdate, medical record number, or government issued identifiers.

Cryptoidentity uses advanced cryptography and information security best practices to enable privacy-compliant data sharing, including:

Single-Use Pseudonymization
Re-hashing all identifying data mixed with random noise for each activity to ensure pseudonyms cannot be leveraged for re-identification.

Differential Privacy
Adding noise to data elements to obscure individual details while maintaining aggregated metrics.

Blind Facilitation
Enlisting a neutral party to determine matches without any computational insight into the de-identification process. This gatekeeper approach blocks the flow of any unmatched data.

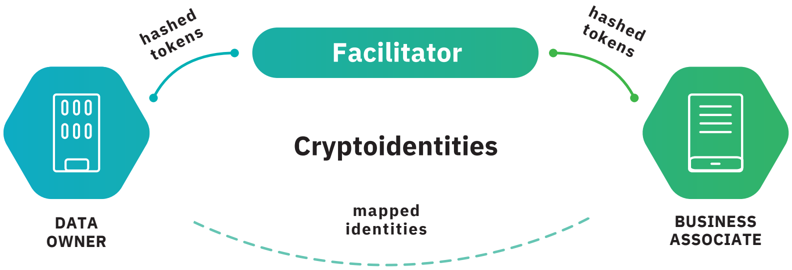
Anonymization
Completely remove all identifying attributes before working with personal data whenever insights can be gained at an aggregate level.

The entirety of this protocol protects against both obvious disclosure and subtle attempts to re-identify the underlying identities. None of the three transaction participants can acquire a new identity that they did not already have direct reference to. In addition, all participants are blind to all identifying information when sharing data.

The future of sharing real-world data: zero trust

Cryptoidentity is the secure data matching foundation of the Karlsgate Identity Exchange™. Data protections are inherent to the platform that users control themselves. No identifiable information ever leaves data owners' internal network and no re-identifiable tokens are released to external parties. Karlsgate Identity Exchange enables data owners to trade their data assets without exposing personal data in a zero-trust environment.

IDs mapped using Karlsgate Identity Exchange



Characteristics

- Non-reusable hashed identifiers used for matching
- Data trading partners can only see their own identifiers
- Mapping rules are obvious to all parties
- Hashed tokens have no identifying value to the facilitator
- No trust is required to ensure protection

Effects On Privacy

- ✓ Underlying identifiers are obfuscated
- ✓ Re-identification is inhibited by blinding the involved parties to the requisite components of the hash algorithm
- ✓ Hashed tokens cannot serve as pseudonymous identifiers since others cannot recompute the token
- ✓ Equitable control over mapping process with enhanced transparency

Security Matrix

Personal data	To the business associate	To the Karlsgate facilitator
Are unknown identities exposed?	No. The facilitator only forwards signals to the trading partner upon a successful match. This prevents disclosure of any new identities to the trading partner.	No. The facilitator only receives hash codes and does not have the full salt value to recreate the hashes.
Can identities be re-identified?	No. Since each participant contributes random noise, retention of the hash value has no re-identifying capacity.	No. The hash codes are constructed with a secret value unknown to the facilitator. There is no worth in matching the resulting hash codes to any other source.

Implementing privacy-by-design data sharing

Karlsgate Identity Exchange solves the biggest issues with sharing insights about patients. It eliminates the need to use unprotected personal identifiers to conduct commerce. This reduces many of the risks that negatively affect personal privacy rights protection without inhibiting the use-cases for data sharing.

Utilizing Karlsgate Identity Exchange supports organizations' plans to build protections directly into their data sharing practices. It is a privacy-by-design data sharing approach that eliminates transferring or disclosing any Personal Data. Using Cryptoidentity to map identities eliminates the need for trust in data sharing partnerships.

No Capacity for Identity Discovery
Cryptoidentity does not permit the acquisition of additional insight or data points regarding any identity not previously present in a participant's data set.

No Personal Revelation
Triple-sourced random initialization vectors and one-way cryptographic hashing techniques create a one-way function, in which the input of the function cannot be inferred or deduced from the output of the function.

No Residual Constancy
Hash values are seeded against later reuse or inference. Single-use, random values mixed into the identifier ensures that no single participant can derive a stable or predictable output from the resultant hash values.

No Identifying Granularity
Individual identities are protected using limiters. Successful identifier mapping is based on a minimum threshold negotiated between the parties prior to uploading hashes with an absolute minimum value of 30.

Karlsgate

Data is the fuel that drives business decisions, powers AI engines, and supercharges healthcare innovation. But harnessing privacy-sensitive, individual-level data poses formidable challenges when it comes to data access, data quality, interoperability, personal privacy, and compliance with ever-evolving security regulations.

Karlsgate enables agile data collaboration at scale, seamlessly connecting data from diverse sources and powering AI learning engines with advanced automation for precision and speed. Sensitive data remains safeguarded during all touchpoints of the data-sharing process, thanks to privacy-enhancing measures embedded directly into data workflows. Learn more about us at karlsgate.com or get in touch at contact@karlsgate.com.

[1] IBM: Cost of a Data Breach Report, 2023. [2] U.S. Department of Health and Human Services. [3] HIPAA Journal: 2022 Healthcare Data Breach Report. [4] Karlsgate Inc.