

CLAIMS:

1. A method for sharing confidential data between a first data provider and a second data provider, the method comprising:

determining a correspondence between one of multiple first data records from the first data provider and one of multiple second data records from the second data provider,

the multiple first data records being stored on a first data store being accessible by the first data provider and protected by encryption from the second data provider, each of the multiple first data records comprising an identifier that references a respective first data record,

the multiple second data records being stored on a second data store being accessible by the second data provider and protected by encryption from the first data provider, each of the multiple second data records comprising an identifier that references a respective second data record; and

creating a third data record on a third data store, the third data record comprising the identifier that references the respective first data record as a first reference to the one of the multiple first data records and the third data record comprising the identifier that references the respective second data record as a second reference to the one of the multiple second data records, wherein

the identifier that references the first data record is accessible by the second data provider and the identifier that references the second data record is accessible by the first data provider.

2. The method of claim 1, further comprising receiving an indication of one or more columns of the first and second data records, wherein determining the correspondence comprises determining a match of values in the one or more columns between the first data records and the second data records.

3. The method of claim 1, further comprising storing one or both of:

in the first data store associated with the one of the multiple first data records an indication of a match type between the one of the multiple first data records and the one of the multiple second data records; and

in the second data store associated with the one of the multiple second data records an indication of a match type between the one of the multiple first data records and the one of the multiple second data records.

4. The method of claim 1, further comprising:
receiving the multiple first data records;
encrypting the multiple first data records to obtain encrypted first data records that are protected from the second data provider; and
storing the encrypted first data records on the first data store.
5. The method of claim 4, wherein
encrypting the multiple first data records comprises using a first symmetric key that is protected from the first data provider and protected from the second data provider, and
the first data records are accessible to the first data provider by checking the first data provider's credentials and decrypting the first data records using the first symmetric key.
6. The method of claim 4, further comprising:
receiving the multiple second data records;
encrypting the multiple second data records to obtain encrypted second data records that are accessible by the second data provider and protected from the first data provider; and
storing the encrypted second data records on the second data store.
7. The method of claim 6, further comprising:

receiving a query value from the first or the second data provider;
encrypting the query value using the first asymmetric key to determine an encrypted query value; and

performing a query for the encrypted query value over the encrypted first data records or the encrypted second data records.

8. The method of claim 4, wherein receiving the multiple first data records comprises:

generating a key pair comprising a public key and a private key;

sending the public key to the first data provider;

receiving from the first data provider an encrypted second symmetric key that is encrypted using the public key;

decrypting the encrypted second symmetric key using the private key;

receiving from the first data provider encrypted first data records that are encrypted using the second symmetric key; and

decrypting the encrypted first data records using the second symmetric key.

9. A non-transitory computer-readable medium with instruction code stored thereon that, when executed by a computer, causes the computer to perform a method for sharing confidential data between a first data provider and a second data provider, by performing the steps of:

determining a correspondence between one of multiple first data records from the first data provider and one of multiple second data records from the second data provider,

the multiple first data records being stored on a first data store being accessible by the first data provider and protected by encryption from the second data provider, each of the multiple first data records comprising an identifier that references a respective first data record,

the multiple second data records being stored on a second data store being accessible by the second data provider and protected by encryption from the first data

provider, each of the multiple second data records comprising an identifier that references a respective second data record; and

creating a third data record on a third data store, the third data record comprising the identifier that references the respective first data record as a first reference to the one of the multiple first data records and the third data record comprising the identifier that references the respective second data record as a second reference to the one of the multiple second data records, wherein

the identifier that references the first data record is accessible by the second data provider and the identifier that references the second data record is accessible by the first data provider.

10. A system for sharing confidential data between a first data provider and a second data provider, the system comprising:

a first data store to store multiple first data records from the first data provider, the first data store being accessible by the first data provider and protected by encryption from the second data provider, each of the multiple first data records comprising an identifier that references a respective first data record;

a second data store to store multiple second data records from the second data provider, the second data store being accessible by the second data provider and protected by encryption from the first data provider, each of the multiple second data records comprising an identifier that references a respective second data record;

a processor having access to the first data store and the second data store to determine a correspondence between one of the multiple first data records and one of the multiple second data records, and

to create a third data record on a third data store, the third data record comprising the identifier that references the respective first data record as a first reference to the one of the multiple first data records and the third data record comprising the identifier that references the respective second data record as a second reference to the one of the second data records, wherein the identifier that references the first data record is accessible by the second data provider and the identifier that references the second data record is accessible by the first data provider.

11. The system of claim 10 further comprising a third data store to store the first reference and the second reference.