

It's Time to 'De-Identify' Your Data

Protect Your Data So You Can Maximize Its Value

Organizations face increasing pressure from regulators and their own customers to fully protect data. The threat of a costly data breach always looms, and businesses have to take their role as data stewards seriously. Yet, effective data security doesn't mean the data has to sit untouched in a vault.

De-identifying your and your customers' data of sensitive elements fully protects the data as it moves across diverse cloud and on-premises environments—enabling your organization to use data to inform AI, machine learning, analytics, and any other data-driven initiative that will help you successfully compete in the digital world.

ORIGINAL DATA

Here's what your data looks like unprotected. It's cleartext.

First Name	Last Name	Email	Gender	SSN	DOB	Diagnosis
Jeffrey	Gordon	Jeffrey.Gordon@meyer.org	M	569-24-058	29/03/1997	Acute bronchitis
Elizabeth	Haynes	EHaynes@axel.org	F	717-37-586	13/08/1985	Coronary Atherosclerosis

PSEUDONYMIZATION: ENCRYPTION AND TOKENIZATION

One method to de-identify this data is pseudonymization. There are two effective ways to pseudonymize: encryption and tokenization.

Encryption uses mathematical algorithms and cryptographic keys to change data into binary cyphertext.

First Name	Last Name	Email	Gender	SSN	DOB	Diagnosis
Y2tpZWxjZmFt==	d29Kc2xmcg==	Zm9vYmFyam9uYmVzQGJpGx5YmlvbmuY29tCg==	M	ndlzLetYl\mYMtM==	PjMvMTlvojkMQo=	Acute bronchitis
H44aa755ronAB==	L3bir3dMvp3==	Am11wAltmah69nr92M Vbos33u2==	F	OPm0IEtAceA mZE==	MtxhDJsc y28JdD=	Coronary Atherosclerosis

Tokenization converts cleartext data into a random string of characters.

First Name	Last Name	Email	Gender	SSN	DOB	Diagnosis
f1RRPef	Zxsepaw	f1RRPef.Zxsepaw@meyer.org	M	569-24-058	22/11/3321	Acute bronchitis
FroifgawM	lCdent	CdeEqI@axel.org	F	717-37-586	10/01/3737	Coronary Atherosclerosis

Pseudonymizing data doesn't mean it's gone forever; the process is reversible, allowing authorized users to view and manage the protected data afterwards. Also, tokenization maintains the same data type; when the user needs the original data, the tokenization system retrieves the original token value, a restoration that can't be accomplished with encryption.

ANONYMIZATION

Anonymization strips sensitive elements from data, irreversibly protecting it.

First Name	Last Name	Email	Gender	SSN	DOB	Diagnosis
*	*	*	M	*	<=1990	Acute bronchitis
*	*	*	F	*	>1990	Coronary Atherosclerosis

Organizations might want to anonymize data for a variety of reasons, especially to participate in data exchanges and marketplaces where data can be shared and monetized. Also, when companies want to share privately company-to-company or with SaaS systems, such as Workday or Salesforce, irreversible protection methods might be required.

MAKE THE MOST OF DATA BY DE-IDENTIFYING SENSITIVE ELEMENTS

- De-identified data is ready to be immediately used in AI, analytics, machine learning, and other business applications without disclosing identities, sensitive personal information, and intellectual property.
- De-identification meets stringent compliance, privacy, and regulatory requirements, including GDPR, PCI, PHI, HIPAA, and PII mandates.
- Data is protected at all times, no matter where it is: cloud and on-premises systems, applications, and files—even if it travels outside to a fully unprotected environment.
- De-identification is compatible with all existing (including Snowflake and Redshift) and future applications, requiring no modification to any code or databases.

PROTECTION ACROSS ALL ENVIRONMENTS

Protegrity secures data where it resides—not just when it is in motion. Rather than creating copies of data or just masking it—leaving the source data vulnerable, as some security platforms do—Protegrity protects *the actual data*. The Protegrity Data Protection Platform closes security gaps and simplifies the management of policies. With a cohesive approach to data protection—including de-identification of sensitive data elements—businesses can extract transformative insights to fuel growth, knowing sensitive data is always secure.

WHY PROTEGRITY

Access to secure data allows companies to generate revenue, innovate, reduce costs, create better products and services faster, comply with regulations, and maintain privacy. Protegrity protects data, no matter where it is, no matter what it is, and no matter how it's used. We protect the world's most secure data, unlocking the potential of secure data to fuel innovation.

It's time to let us help you de-identify your data today.

PROTEGRITY

Protegrity USA, Inc.

(Global Headquarters)
1165 E Wilmington Avenue
Suite 200
Salt Lake City, Utah 84106
1.203.326.7200
1.650.431.7000

Protegrity (Europe)

1 St Katherine's Way
London, E1W 1UN
+44 1494 857762

Email: info@protegrity.com