

- Discover, Classify, Score Re-ID Risk
- Encrypt, Pseudonymize, Redact, etc
- Comply with HIPAA, PCI, GDPR, etc.
- Log, Integrate, Share & Secure Jobs

De-Identification of Sensitive Data



Product Summary

Data privacy law compliance, data breach nullification, and test data safety are critical elements of modern data governance. Securing information is a multifaceted problem that involves: 1) business rules and regulatory environments, 2) identifying sensitive data and its authorized recipients, and 3) de-identifying that data and auditing all activities that support these aims.

What Does FieldShield Do?

IRI FieldShield supports the risk and controls framework in corporate and government IT environments by classifying, finding, masking, risk-scoring, and auditing sensitive data in database tables, flat files, and other legacy and modern data sources. FieldShield quickly and securely obfuscates data at the field level, before it leaves the firewall. FieldShield is used to secure:

- **Personally Identifiable Information (PII)** that reveals someone directly, or in combination with other data.
- **Protected Health Information (PHI)** that identifies someone from a medical record or a designated data set that was created, used, or disclosed in the course of providing a health care service.
- Payment Card Industry Data (PCI), that credit card payments generate, and is thus subject to hacking, fraud, etc.

FieldShield encrypts, masks, or otherwise anonymizes this data according to business rules and privacy laws.

How Does FieldShield Work?

FieldShield locates and categorizes CSI, PI, PII, PHI, PAN and other private data in structured sources with built-in data classification, profiling and search tools. You can then assign specific protections to mask each element, i.e., you can:

- Encrypt with built-in, or your own, libraries
- Filter or mask values, columns, or rows conditionally
- Redact via obfuscating characters or string manipulation
- Pseudonymize, hash, shuffle, randomize, blur, bucket, etc.

FieldShield jobs run in a free graphical IDE built on Eclipse called IRI Workbench, on the command line, and from within batch or application programs. To preserve referential integrity, you can secure like columns across multiple tables in one pass using masking functions that you define or import from a rules library. An XML audit log with all job and runtime details shows the data protections applied to verify compliance with data privacy regulations.

You can also use FieldShield encryption, hashing, and redaction functions for dynamic data masking or unmasking work. The FieldShield software development kit (SDK) supports and documents these API calls in C/C++, Java, and .NET.

Encryption and Decryption Functions

Among FieldShield's many data-centric protection functions are powerful encryption and decryption routines:

- **AES-128 or 256** Displays expanded ciphertext fields as printable ASCII characters
- **3DES** Uses public key ring files
- GPG/PGP Works with GPG key ring management and does not retain the input format
- OpenSSL Conforms to the FIPS 140-2 computer security standard
- Format-Preserving Retains the original width and alpha-numeric field (column) format
- Width-Preserving Retains the original field width, but not the original data format
- Custom Algorithms Supports any function you write or link to that protects data in that field

Symmetric encryption keys can be: 1) held within job scripts as passphrases or environment variables; 2) embedded in secured files (on secured servers); or, 3) remain invisible (by default). Store asymmetric (public) encryption and (private) decryption keys in central key ring servers. HSM and key vault support is via MS Azure or Townsend Alliance Key Manager.

Running FieldShield in Database Environments

FieldShield connects to any RDBMS (SQL) database at rest or in-motion, and runs data masking jobs:

- from the command line, batch program or job scheduler
- in its Eclipse IDE: IRI Workbench including within IRI Voracity ETL jobs and IRI Ripcurrent real-time DB ops
- through a system call, or API call from a C++, Java, or .NET program
- in situ, via SQL procedures using a custom library

What are the Technical Advantages of FieldShield?

Though many physical and broad-brush logical security solutions are available, the wrong design or execution choice reduces performance and leaves data vulnerable to privacy breaches. By contrast, FieldShield delivers:

- Efficiency speeds protection by targeting only sensitive data
- Simplicity requires only one job for multiple protections and recipients
- Security supports different security functions or encryption keys for each field
- Flexibility allows masking and unmasking based on data values or authorization
- Clarity Uses a familiar Eclipse GUI and self-documenting 4GL to define data layouts and protection function

What are the Business Benefits of FieldShield?

FieldShield helps CDOs and CISOs adhere to both business rules and privacy laws in a data-centric context. Some fields remain clear, while others are secured. With FieldShield:

- PII is automatically (or manually) found and classified
- Data are protected at sources and endpoints with multiple functions
- Data stays safe even if it is stolen, or if a laptop or network is decrypted
- Protected data can retain realism for testing, sharing, and database subsetting
- Implementation and maintenance is easier than with DB-specific column encryption
- A query-ready XML audit log helps to verify compliance with data privacy regulations

What else? File and table-specific data profiling, ERDs, and fuzzy search, plus schema-wide data class and pattern search to help you organize and find PII everywhere. The ability to send output to multiple targets simultaneously provides for the separate data masking functions and custom-formatted output to recipients with different authorizations and needs. The graphical multi-table protection wizards mask like columns across tables in the same way, saving multiple design steps, I/O passes, data synchronization errors, and referential integrity. Peer-reviewed statistical re-ID risk scoring and anonymization facilities combine to render data compliant with FERPA and HIPAA regulations, but still valuable for marketing and research.

What are Some Data Sources FieldShield Protects?

Standard

- CSV / Delimited
- Fixed & Fixed Block
- Excel, JSON, LDIF & XML
- Line, Record, Variable Sequential
- Micro Focus Variable Length & ISAM
- Oracle, DB2, MS SQL, MySQL
- Ingres, PostgreSQL, Sybase
- SAP HANA, Snowflake, Teradata

Cloud, Hadoop, NoSQL

- Amazon Redshift, RDS, etc.
- Cloudera CDH & Impala
- Google BigQuery
- Hortonworks & MapR HIVE
- MS SQL Azure
- NoSQL (Cassandra & MongoDB)
- Pivotal (Greenplum, HIVE)
- Salesforce

Legacy*

- Adabas
- ASN.1 CDRs
- C-ISAM Informix
- D-ISAM
- dBase
- Datacom & DataFlex
- IDMS & IMS
- Unidata

* may require IRI-partner drivers

What Applications are Compatible with FieldShield?

FieldShield runs on UNIX, Linux, and Windows, masking data in the databases and file formats they support, plus mainframe, Hadoop, some NoSQL, and SaaS platforms. FieldShield is also compatible with the metadata or masking functions used by:

- IRI Voracity the big data management platform that includes FieldShield, DB subsetting, and:
- IRI CellShield EE for masking data in Excel
- IRI DarkShield for masking semi- and unstructured data
- IRI RowGen for synthesizing intelligent test data
- IRI CoSort for data transformation, cleansing, wrangling and reporting
- IRI NextForm for data, file, and database conversion and replication

FieldShield data definition file (.ddf) format is also supported by DataSwitch and Value Labs Test Data Hub, plus:

- erwin (Quest) Mapping Manager & Smart Connectors
- MITI Meta Integration Model Bridge

These tools facilitate the creation or conversion of third-party ETL, BI, and modeling tool metadata into FieldShield metadata, so that you can accelerate the building of data masking jobs for the sensitive columns already defined in those environments.

FieldShield is also certified to run in conjunction with database cloning software from Actifio, Commvault and Windocks.

FieldShield-Supported Platforms

- UNIX (AIX, HP-UX, Solaris)
- Linux on x86, Itanium, IBM s/p/i/z
- macOS
- Microsoft Windows

FieldShield in IRI Workbench

FieldShield users leverage a free Eclipse plug-in to create, run, and manage data protection jobs. This graphical user interface supports all data classification, search, and masking activities. Multiple methods support target format control.

and the second se		and the second se	Tiew Field Rule Wo	Card Development and Carden
Encryption and Decryption Functions		Window and Ja	New Protection Fie	eld Rule Wizard Selection
neryption and Decryption Functions		345	Create encoding or decoding functions.	
epulate arguments as specified in the inst	nuctions. Optional arguments are in brackats. The green chack m	WAR OF A		
tent with these at the			a S Protection R	ules sent funcession fluider
epression: enc_aes256(\$(FIELDMAAME))		1	De-identi	sty or Re-identify Function
Encryption and Decryption Function * Function name: enr.,ses256			The Encoding or Decoding Functions	
ing lates, etc. (Kehl generatives)	Jues AES 256-bit encryption to encrypt a field.Every 3 bytes will be	e replaced with 4	// Hashing	functions
les_lides_ssl(tietd.passphrase)	invitable characters. This results in a further 314 expansion of the f	held som.	60 Masking	Function
iec_aes128(field.passphrase)	The passphrase can be a string, environment variable, or a referen	ce to a file name	Random C	ym Replacement Value Generation
iec_aes256 (field pacephrase) 4 iec_aes256_stiffield pacephrase)	end path. No argument - a secret, internal passphrase is used.	985 H.S. (2011) (1	fx String Ma	anipulation Functions
lec. fp. aes256_elphanum(lield,passphi	Provide and a second seco			1 SNR CONTRACTOR
Sec. fp., sec256, accidited, parcphrase, ev	Sector Carrier Active Control of		A Real Property of The	additional Foreigne
lec_fp_kes256_ascx_stiffield,passphras lec_gpg(field,key80,path)	Paraphrana []		Lineary Incarion The	
enc_3des_ebc(field.passphrase) enc_3des_ssl(field.passphrase) enc_aes128(field.passphrase)	m New Multi-Table Protect Job	1	Liteary harnel	Laborary Factorians
	Field Modification Sular		Pure name: Em	xeeingRute
mc_aes128_ssifteein.passphrase	Add and remove field modification rules.		Overwrite existing	Mesking Function In Solution
ne aes256 solfield passphrase)				Masking Function
mc_fp_ses256_elphanum_ssl/field.pesc	Table nations into?			Replaces a range of characters in the required source field with a replacement
enc. fp. am256 micii stilfield passphras	Remove Ables has been being to starting			Charles .
spg(held.teg@.path)	ramon of the lack for the factor of the		3	Source field S(RELDNAME)
	Test far matches	in the second	C.	
	Rule Name EncodingRule Details EXPRESSION e en	scode_hase64(\$(FB	ELDPEAME]], NAN Boom	Use predefined masks
	Add to table			Predefined Masks
90	North Ration Rule Ton	Databa		Mask Example (0)(E23456780 == ********
~	EncodingRule \b[\w_N+_ ENC.864 EXPRESSION	EXPRESSION	N = encode_baseb#cScFitt	Made Whole Field
			New Contraction of the	Credit Card
Target Field Layout				Canada SIN
lap and modify target data leyouts. Use th	e right-click context menu to edit fields and apply field rules.	E Pseudonym B	aplacement	Arguer Chile RUT
euri ini		Pseudonym Re	placement Field Rule	Finland PIN
(Prince)		Create a poeside	onym field that will use v	Hong Kong MD Iceland Pilv
Field Field Name	Data Type Position Size Additional Attributes	aniginal field's v	values.	Korea SSN
Dimporte RecType	ASCII I 0 Separator]	Preudonymize	field STELDNAMD	Type Singapore NPDC
Simporte. EmployeeHRID	ASCE 2 0 Separator			Sweden PIN
Imports. EffectiveDate	ASCE 3 0 Separator 1	· Use provided	I presidencym list (men-re	Switzerland PD4
•		Name options		UK NINO
argets:		Name type: 1	First +	
MaskedEPs		Sec 1	Male +	
9 1 B M		Orden I	First and Last +	
Delimiter		Defect structure int file. CORP.Co.		
Proved a Detremented Separature 1	Trame	The only of	nime names from mand	
Field Field Narve	Data Type Position Additional Attributes	(Blanks inse	ented when # of records in	(?) . Back Next - Finish Cancel
G Field RECTVPE	ASCB 1 Separator)			
Field EMPLOYEEHIER	AGCIE 2 Separatori	C Der vour own	n posudonum list inon-m	recoverable)
Gillet PSEUDO_EMP Inser	t Below + 4 Separator Set "C:/RD/Cullort	User pseudony	ym lat.	
Set PSEUDO_EMP	Rute + Browin Rule	Paratherpentis	1914	Department (
Pieta EMPLOYEEME	Create Rule.	C Use original	finitian a look-up one p	planutorym tut
× Sam	eve .	@ Une Landon	n draw friters proceditingers	a Sud
		Use only a	unique names from poes	udoriym Bill
2		(Diseky bu)	artain when Worf respirate	is greater these # of series and series ()
	OK E	(Stanky ou	artais when Wild incode	in generation was a straining marked
0		Ð	Sect.	First - Final Canad
T		Ð	(< Back)	Next > Finish Cancal
3		Ŷ	. s Back	Next : Finish Concel
3		٢	[< Back]	Page s Finish Cancel
3		۲	(6ack)	Rept: 1 Finish Cancel
3		•	- Back	Paper > Finish Cancel

© 2025 Innovative Routines International (IRI), Inc. All Rights Reserved. CoSort, Voracity, NextForm, FieldShield, CellShield, DarkShield, and RowGen are trademarks or registered trademarks of IRI. FACT is a trademark of DataStreams Corp. (CoSort Korea). Other product, brand, or company names may be (registered) trademarks of their respective holders.

Total Data Management

/ | | \ |

2194 Highway A1A Melbourne, FL 32937 USA 1.321.777.8889 * 1.800.333.SORT

