IRI FieldShield
PII / PHI Classification & Masking

- Discover, Classify, and Apply Rules to PII
- Encrypt, Pseudonymize, Redact, etc.
- Comply with HIPAA, PCI, GDPR, etc.
- Log, Integrate, and Share Jobs

De-Identification of Sensitive Data

Product Summary

Data loss prevention and the protection of sensitive information are critical elements of modern data governance. Safeguarding data at risk is a multifaceted problem that requires: 1) knowledge of business and regulatory requirements, 2) classification of sensitive data and its authorized recipients, and 3) implementation of policies and techniques that support these requirements.

What Does FieldShield Do?

IRI FieldShield supports the risk and controls framework in corporate and government IT environments by finding and masking sensitive data in relational database tables, flat-files, and many other legacy and modern data sources. FieldShield quickly and effectively obfuscates data in these repositories - down to the field level - before it leaves the firewall. FieldShield can secure:

- **Personally Identifiable Information (PII)** that reveals someone directly, or in combination with other data.
- **Protected Health Information (PHI)** that indentifies someone from a medical record or a designated record 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 PII, PHI, or PCI in disparate sources with onboard data profiling and classification tools. You can then assign specific protections to de-identify each element:

- Encrypt with built-in, or your own, libraries
- Filter columns or redact rows based on conditions
- Mask via obfuscating characters or string manipulations
- Pseudonymize, hash, shuffle, or randomize

FieldShield jobs run in the IRI Workbench GUI, on the command line, or from within batch and 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 in dynamic data masking, Hadoop, and database applications. The FieldShield software development kit (SDK) supports and documents API calls in C/C++, Java, and .NET.

Encryption and Decryption Options

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. Obtain HSM support through custom development.

Running FieldShield in Database Environments

FieldShield connects to database data at rest or in-motion, and runs:

- On the command line or batch
- From the Eclipse GUI: IRI Workbench
- Through a system, 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 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 DB-specific column encryption
- A query-ready XML audit log helps to verify compliance with data privacy regulations

In one pass, FieldShield can produce one or more targets for recipients with different authorizations. The multi-table protection wizard in the GUI masks like columns across tables in the same way. This saves multiple passes through the data, prevents data synchronization errors, and preserves referential integrity.

What Are Some Data Sources FieldShield Protects?

Standard

- CSV
- Delimited
- Fixed Block File Format
- LDIF
- Line, Record, Variable Sequential
- MicroFocus Variable Length & ISAM
- RDBMS (Oracle, DB2, MySQL, SQL Server, PostgreSQL, Sybase, Teradata)
- Text
- XML

Legacy

- Adabas
- C-ISAM Informix, D-ISAM
- Datacom
- DataFlex
- dBase
- IDMS
- IMS
- Intersystems
- PostgresSQL
- Unidata

Modern

- Amazon EMR, RDS, etc.
- Cloudera CDH & Impala
- Hortonworks Hive
- MapR Hive
- MS SQL Azure
- NoSQL (Cassandra & MongoDB)
- Pivotal (Greenplum, Hive)
- Spark SQL
- Web-based (Eloqua, Hubspot, Marketo, SalesForce, etc.)

What Applications are Compatible with FieldShield?

FieldShield runs on UNIX, Linux, and Windows, and operates on the databases and file formats they support, plus mainframe, Hadoop, NoSQL, and SaaS platforms. FieldShield uses the same metadata as:

- AnalytiX DS - Mapping Manager
- IRI CellShield - Data Masking for Excel
- IRI CoSort - Data Integration & Transformation
- IRI FACT - Fast Extract for Oracle, DB2, et al.
- IRI NextForm - Data and Database Conversion
- IRI RowGen - Realistic Test Data Generation
- IRI Voracity - Total Data Management
- MITI - Meta Integration Model Bridge

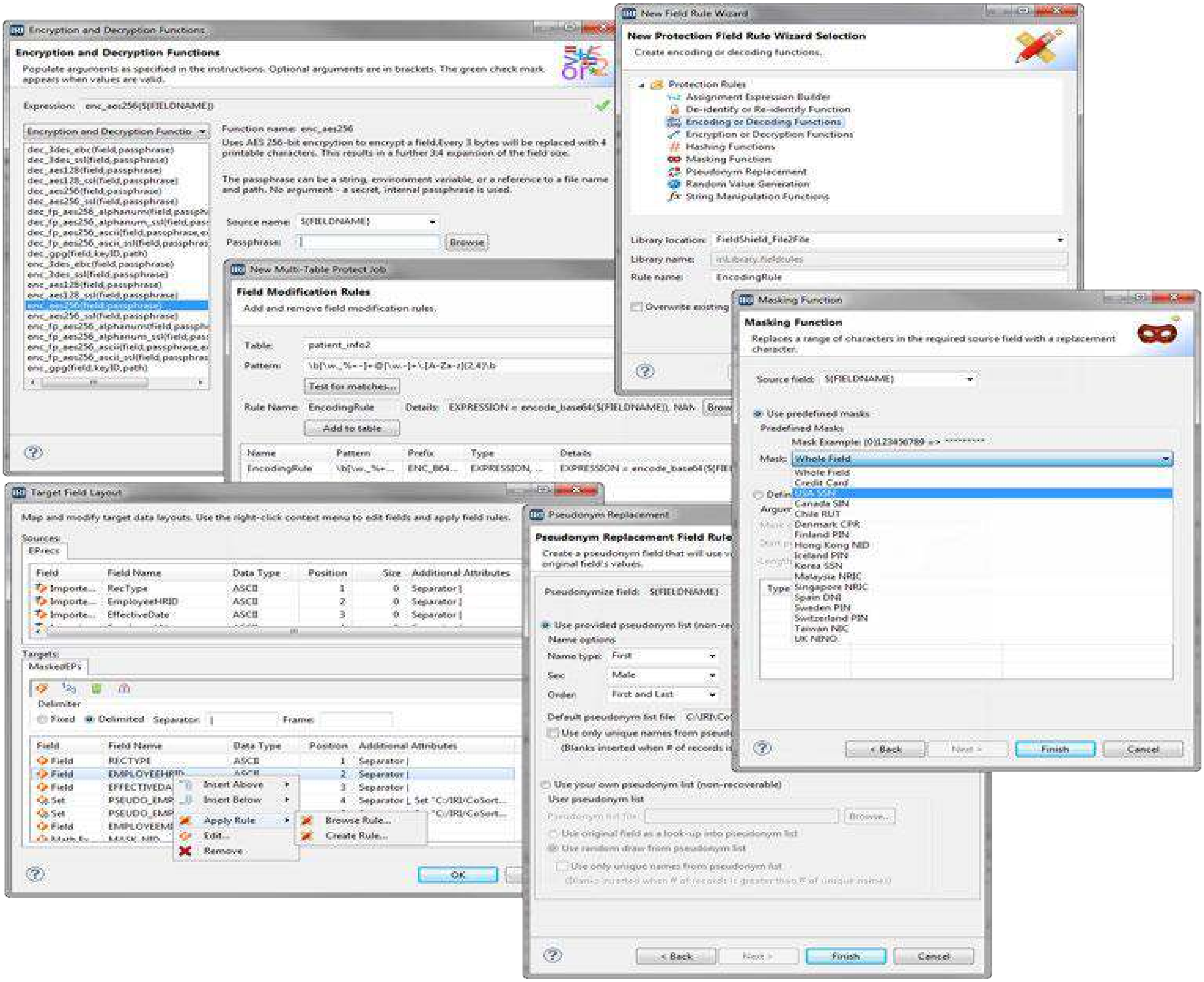
FieldShield's data definition file (.ddf) format is interchangeable with all IRI products, and supported by popular metadata exchange hubs. They facilitate the conversion of third-party ETL, BI, and modeling tool metadata into FieldShield metadata so that you can more rapidly protect sensitive data in those environments.

FieldShield-Supported Platforms

- UNIX (AIX, HP-UX, Solaris, Tru64 & more)
- Linux on x86, Itanium, IBM s/p/i/z, FreeBSD
- Windows® (XP, 2000-2016, 7, 8, 10)
- MacOS (Sierra)

FieldShield in the IRI Workbench

FieldShield users get a free Eclipse plug-in to create, run, and manage data protection jobs. The GUI supports nine of FieldShield's twelve categories of protection functions. The output field layout editor controls the formatting of every target.



Encryption and Decryption Functions

Populate arguments as specified in the instructions. Optional arguments are in brackets. The green check mark appears when values are valid.

Expression: enc_aes256(${FIELDNAME})

Function name: enc_aes256

Uses AES 256-bit encrpytion to encrypt a field.Every 3 bytes will be replaced with 4 printable characters. This results in a further 3:4 expansion of the field size.

The passphrase can be a string, environment variable, or a reference to a file name and path. No argument - a secret, internal passphrase is used.

Source name: ${FIELDNAME}

Passphrase:

Encryption and Decryption Functio
dec_3des_ebc(field,passphrase)
dec_3des_ssl(field,passphrase)
dec_aes128(field,passphrase)
dec_aes128_ssl(field,passphrase)
dec_aes256(field,passphrase)
dec_aes256_ssl(field,passphrase)
dec_fp_aes256_alphanum(field,passph
dec_fp_aes256_alphanum_ssl(field,pass
dec_fp_aes256_ascii(field,passphrase,e
dec_fp_aes256_ascii_ssl(field,passphras
dec_gpg(field,keyID,path)
enc_3des_ebc(field,passphrase)
enc_3des_ssl(field,passphrase)
enc_aes128(field,passphrase)
enc_aes128_ssl(field,passphrase)
enc_aes256(field,passphrase)
enc_aes256_ssl(field,passphrase)
enc_fp_aes256_alphanum(field,passphr
enc_fp_aes256_alphanum_ssl(field,pass
enc_fp_aes256_ascii(field,passphrase,e
enc_fp_aes256_ascii_ssl(field,passphras
enc_gpg(field,keyID,path)
Browse

New Multi-Table Protect Job

Field Modification Rules

Add and remove field modification rules.

Table: patient_info2

Pattern: \b[\w._%+-]+@[\w.-]+\.[A-Za-z]{2,4}\b

Rule Name: EncodingRule

Details: EXPRESSION = encode_base64(${FIELDNAME}), NAM

Name	Pattern	Prefix	Type	Details
EncodingRule	\b[\w._%+-...	ENC_B64...	EXPRESSION, ...	EXPRESSION = encode_base64(${FIEL

New Field Rule Wizard

New Protection Field Rule Wizard Selection

Create encoding or decoding functions.

Protection Rules
Assignment Expression Builder
De-identify or Re-identify Function
Encoding or Decoding Functions
Encryption or Decryption Functions
Hashing Functions
Masking Function
Pseudonym Replacement
Random Value Generation
String Manipulation Functions

Library location: FieldShield_File2File

Library name: iri\Library.fieldrules

Rule name: EncodingRule

□ Overwrite existing

Masking Function

Replaces a range of characters in the required source field with a replacement character.

Source field: ${FIELDNAME}

● Use predefined masks

Predefined Masks

Mask Example: (0)123456789 => *********

Mask: Whole Field

Target Field Layout

Map and modify target data layouts. Use the right-click context menu to edit fields and apply field rules.

Sources: EPrecs

Field	Field Name	Data Type	Position	Size	Additional Attributes
Importe...	RecType	ASCII	1	0	Separator |
Importe...	EmployeeHRID	ASCII	2	0	Separator |
Importe...	EffectiveDate	ASCII	3	0	Separator |

Targets: MaskedEPs

Delimiter ○ Fixed ● Delimited Separator: | Frame:

Field	Field Name	Data Type	Position	Additional Attributes
Field	RECTYPE	ASCII	1	Separator |
Field	EMPLOYEEHRID	ASCII	2	Separator |
Field	EFFECTIVEDA		3	Separator |
Set	PSEUDO_EMP		4	Separator |, Set "C:/IRI/CoSort...
Set	PSEUDO_EMP			"C:/IRI/CoSort...
Field	EMPLOYEEME			
Math Ex...	MASK_NID			

Pseudonym Replacement

Pseudonym Replacement Field Rule

Create a pseudonym field that will use v original field's values.

Pseudonymize field: ${FIELDNAME}

● Use provided pseudonym list (non-re

Name options

Name type: First

Sex: Male

Order: First and Last

Default pseudonym list file: C:\IRI\Co

□ Use only unique names from pseudo

(Blanks inserted when # of records i

○ Use your own pseudonym list (non-recoverable)

User pseudonym list

Pseudonym list file:

○ Use original field as a look-up into pseudonym list

● Use random draw from pseudonym list

□ Use only unique names from pseudonym list

(Blanks inserted when # of records is greater than # of unique names)

IRI Total Data Management | CELEBRATING 40 YEARS 2018 The CoSort Company

2194 Highway A1A, 3rd Floor
Melbourne, FL 32937 USA
1.321.777.8889 ⁕ 1.800.333.SORT

WWW.IRI.COM