PII Field Encryption Considerations

CAREWare's built-in PII software encryption was added several years ago, at a time when the security landscape was different and broader system-level encryption options were not as commonly available.

CAREWare's built-in PII software encryption is not scheduled for updates and is not a complete encryption-at-rest solution for CAREWare. jProg plans to remove CAREWare's built-in PII software encryption in the future.

jProg recommends that organizations work with their local IT and security teams to follow their own policies for protecting PII and encryption at rest. This includes cw_data, all other CAREWare databases, attachments, transaction logs, backups, and the server drive itself.

As part of that review, local IT and security teams may also want to consider related safeguards, such as server access, database permissions, administrative accounts, patching, endpoint protection, firewall rules, audit logging, and backup security.

Once those local security policies are in place, jProg recommends turning off CAREWare's built-in PII encryption option.

Purpose	Help CAREWare administrators understand PII encryption settings, plan changes, and verify that encryption or decryption is complete.
Who should do this	CAREWare administrators, DBAs, and local IT or security staff responsible for SQL Server and privacy safeguards.
Use this guide when you need to	Confirm the PII encryption state, plan a migration or test refresh, temporarily decrypt for approved DBA work, or turn encryption back on.
Main warning	CAREWare's built-in PII Encryption is not a complete or modern encryption solution and will be removed in a future build. It will also reduce CAREWare performance. Working with local IT guidance, users should transition away from CAREWare's built-in PII Encryption as soon as possible.
Compliance reminder	CAREWare PII encryption is one control. Local IT remains responsible for data at rest, backups, transport security, access control, and HIPAA documentation.

Quick path

CW Admin Utility > Stop Server > LocalNumberStorage > EncryptPIIFields > Edit > set 1 to encrypt or 0 to decrypt > Save > Start Server.

Before you begin

PII field encryption changes should be planned as a maintenance task, not handled during normal user activity.

- Review your organization's HIPAA, privacy, and data-at-rest policy before changing encryption settings.
- Create a current CAREWare database backup and record the current EncryptPIIFields and PIIFieldsEncrypted values.
- Schedule downtime and have all users log out before the Business Tier service is stopped or encryption processing begins.
- Use a test environment first to review the process before making changes to the production database.

How CAREWare PII encryption works

CAREWare can encrypt PII fields in SQL for the cw_client and cw_map_client_provider tables. These fields include client name, DOB, address, and similar client-identifying values. When encrypted, those fields appear as null values in SQL queries.

Setting	What it means
EncryptPIIFields	CAREWare Business Tier action setting in LocalNumberStorage. Set to 1 to encrypt decrypted PII fields. Set to 0 to decrypt encrypted PII fields.
PIIFieldsEncrypted	Common Storage state flag. 1 means the database is already encrypted. 0 means it is already decrypted.

Tip

Only change EncryptPIIFields in the CW Admin Utility unless the CAREWare Help Desk directs you to change the Common Storage state flag. A mismatch can occur after migration or when a test environment is refreshed from production.

Expected setting combinations

EncryptPIIFields	PIIFieldsEncrypted	Result
1	1	PII fields are encrypted. CAREWare takes no action.
0	0	PII fields are decrypted. CAREWare takes no action.
1	0	CAREWare begins encrypting decrypted PII fields.
0	1	CAREWare begins decrypting encrypted PII fields.

Change the CAREWare action setting

Step 1. Go to C:\Program Files\CAREWare Business Tier, right-click CW Admin, and click Run as Administrator.

Step 2. Click Stop Server.

Step 3. Select LocalNumberStorage under TableName, then select EncryptPIIFields.

Step 4. Click Edit and set the value to 1 to encrypt PII fields, or 0 to decrypt PII fields.

Step 5. If EncryptPIIFields is missing, click Add, enter EncryptPIIFields as the Tag, and enter 1 or 0 as the Setting.

Step 6. Click Start Server and wait for the process to complete before users return to CAREWare.

Confirm it worked

Run the applicable SQL query against cw_data. When records are encrypted, these PII columns appear as null. When records are decrypted, they appear as not null.

```
USE cw_data;
SELECT cln_last_name FROM cw_client WHERE cln_last_name IS NULL;
SELECT map_cln_last_name FROM cw_map_client_provider WHERE map_cln_last_name IS NULL;
```

For the decrypted state, change IS NULL to IS NOT NULL. During decryption, the null results should decrease until none remain. During encryption, the not-null results should decrease until none remain.

Important

Keep users out until verification is complete. While CAREWare is changing the PII state, affected clients can appear missing from Find Client results.

Migration and test-refresh reminders

- Before migrating CAREWare to a new server, record both EncryptPIIFields and PIIFieldsEncrypted.
- Before restoring a test environment from production, remember that cw_common_storage can be replaced by production values.
- If the Business Tier action setting and database state flag do not match the real PII state, stop and contact the CAREWare Help Desk before editing Common Storage directly.

When to contact Help Desk

- You are not sure whether the database is actually encrypted or decrypted.
- PIIFieldsEncrypted appears wrong or conflicts with observed query results.
- Users cannot find clients after processing should have completed.
- You need to change Common Storage directly or recover from a migration/test-refresh mismatch.

References

CW Admin Utility Decrypt cw_map table Common Storage Values Test Server refresh process