# 3. Sensitive data exposure

Sensitive information, such as personally identifiable information (PII), medical data, and financial records, must be safeguarded by the application to prevent data theft and malicious modification, and unintentional unauthorized access and accidental modification. Applications should be designed and developed to utilize robust access control management and industry-recognized encryption algorithms with encryption key management functionality, to ensure sensitive data is protected while **in transit and while at rest**, including when data is exchanged between the application and a user’s web browser.

Data Classification →

All tables

Fields Business Owner Compliance (GDPR, CCPA)

Encryption - In database - Rotate keys -

PII Data → search

Exact match→ Deterministic Encryption: SS NO

Credit card→ Probabilistic encryption

Audit Trail - At the field level

Lower environments —--> Scrub data test data

SSL between Server and Client

To ensure applications are developed with the appropriate level of security and functionality to prevent sensitive data exposure within the Software Development Lifecycle’s design stage, include a sensitive data impact assessment.

## GDPR Compliance

## Sensitive data impact assessment

A sensitive data impact assessment starts with documenting and evaluating all the data that is intended to be accessed and processed by the application, and then assigning a data type classification (such as personal data, financial data). Following this, the application’s security controls and functions should be reviewed by a subject matter expert for each data classification identified. For instance, if the application is intended to process PII, the review should involve either a Data Privacy Officer or a data protection legal expert to ensure the application’s security controls and measures complies with data protection laws — which, in the case of data protection, varies from country to country.